- Сектор за правни работи -

Архивски број: 03-12343/1
Датум: 29.11.2022

Друштво за професионални и консултантски услуги
ТЕЛЕЛИНК БИЗНИС СЕРВИСИС ДООЕЛ
Бр. 03-190/1
29.11.2022 год.
СКОПЈЕ

ДОГОВОР
за јавна набавка на стоки - управување со привилегиран пристап (PAM)

Склучен помеѓу:

1. МИНИСТЕРСТВО ЗА ФИНАНСИИ, со седиште на ул. Даме Груев бр.12 - Скопје, претставувано од Dr.Fatmir Besimi, министер за финансии, во натамошниот текст: договорен орган

и

2. Друштво за професионални и консултантски услуги ТЕЛЕЛИНК БИЗНИС СЕРВИСИС ДООЕЛ Скопје, со седиште на Ул. Фјодор Достоевски бр.72, вл.1 кат 4/ стан 5 - Скопје, претставувано од Боби Цветковски, управител во натамошниот текст: носител на набавката.

I. ПРЕДМЕТ НА ДОГОВОРОТ

Член 1

Предмет на договорот е јавна набавка на стоки – управување со привилегиран пристап (PAM), согласно со техничките спецификации (Прилог 1) и понудата на носителот на набавката прифатена од страна на договорниот орган, кои се составен дел од овој договор, а по претходно спроведена поедноставена отворена постапка, по оглас број бр.17338/2022.

Називот на системот за управување со привилегиран пристап гласи: CyberArk Privileged Acess Management.

II. ВРЕДНОСТ НА ДОГОВОРОТ

Член 2

Вкупната вредност на договорот без пресметан данок на додадена вредност изнесува 1.890.000,00 денари.

Вкупниот износ на данок на додадена вредност изнесува 340.200,00 денари.

Вкупната вредност на договорот со пресметан данок на додадена вредност изнесува 2.230.200,00 денари.

III. РАЗЛИКА ВО ЦЕНА (КОРЕКЦИЈА НА ЦЕНИ)

Член 3

Цената од член 2 на овој договор е крајна, фиксна и непроменлива за цело времетраење на договорот.

IV. РОК НА ВАЖНОСТ НА ДОГОВОРОТ

Член 4

Овој договор се склучува за период од 12 (дванаесет)месеци, а ќе започне да важи од денот на потпишувањето од двете договорни страни.

V. НАЧИН, МЕСТО И РОК НА ИСПОРАКА

Член 5

Носителот на набавката е должен предметот на договорот да го изврши во согласност со техничките спецификации, потребите и барањата на договорниот орган и во рок кој ќе го определи договорниот орган во писмена порачка која ќе биде испратена до носителот на набавката.

Носителот на набавката е должен за испорака на предметот на набавка да издаде Работен налог / Извештај / Записник, кој мора да ги содржи податоци за испорака на предметот на договорот.

Работниот налог / Извештај / Записник за извршената испорака односно инсталација и ставање во упротреба на системот, со полно име и презиме го потпишуваат определените лица од двете договорните страни, при што по еден примерок се предава на задолженото лице кај договорниот орган, еден примерок задржува носителот на набавката за сопствени потреби и еден примерок заедно со фактурата се доставува до Министерството за финансии - Скопје.

Испораката на предметот на договорот ќе се врши во просториите на договорниот орган во Скопје.

VI. НАЧИН И РОК НА ПЛАЌАЊЕ

Член 6

Договорниот орган плаќањето ќе го изврши во рок до 30 (триесет) дена од денот на доставувањето на фактурата за испорака на предметот на набавка, во писарницата на Министерството за финансии на ул. „Даме Груев" бр.12 во Скопје.

- Сектор за правни работи -

Кон фактурата носителот на набавката задолжително доставува Работен налог / Извештај / Записник кој мора да ги содржи податоци за испорака односно инсталација и ставање во употреба на системот, во спротивно фактурата нема да биде платена и ќе биде вратена на докомплетирање кај носителот на набавката.

Фактурата се доставува по пошта или лично во писарницата на Министерството за финансии, на ул. Даме Груев бр.12 во Скопје.

VII. ПРАВА И ОБВРСКИ НА НОСИТЕЛОТ НА НАБАВКАТА

Член 7

Носителот на набавката е должен да достави претплата за 10-25 администратори за период од 12 (дванаесет) месеци и да обезбеди минимум од следните функционалности согласно со техничките спецификации при што сите функционалности мора да бидат обезбедени од истиот производител:

- управување со корисници и привилегиран пристап;
- заштита од далечински пристап;
- мулти-факторска автентикација и обезбедување пристап до клучните апликации преку порталот Single Sign-On.

Член 8

Носителот на набавката е особено должен:

- да обезбеди ефикасно и навремено извршување на договорот и да ги применува соодветните регулативи за конкретниот вид на стоки придржувајќи се кон барањата нагласени од договорниот орган;
- да дава соодветни препораки за решавање на секој проблем кој би се појавил во текот на реализација на предметниот договор;
- да му се укаже на договорниот орган за било која неправилност во врска со непочитувањето на законската регулатива или било кој друг факт кој би можел негативно да влијае на исходот или очекувањата на договорниот орган;
- да пристапи кон извршување на предметот на договорот по приемот на барањето од договорниот орган за набавка;
- во рамките на извршувањето на своите обврски блиску да соработува со вработените кај договорниот орган кои ќе бидат задолжени за реализација на предметниот договор.

Носителот на набавката се обврзува и е должен во рамките на извршувањето на своите обврски да ги смета барањата и интересите на договорниот орган кои се предмет на овој договор за приоритетни во секое време и да го информира договорниот орган, веднаш доколку се појават одредени околности кои би влијаеле на извршувањето на активностите кои се предмет на овој договор.

VIII. ПРАВА И ОБВРСКИ НА ДОГОВОРНИОТ ОРГАН

Член 9

Договорниот орган е должен да определи лица задолжени за реализација на договорот и за истото да го извести носителот на набавката.

Договорниот орган е должен да достави писмено барање (порачка) со точни спецификации и барања со цел да се изврши реализација на договорот.

Договорниот орган се обврзува дека плаќањето на носителот на набавката ќе го изврши во рокот од членот 6 на овој договор.

IX. ГАРАНЦИЈА ЗА КВАЛИТЕТНО И НАВРЕМЕНО ИЗВРШУВАЊЕ НА ДОГОВОРОТ

Член 10

Носителот на набавката е должен заедно со потпишаниот договор да достави банкарска гаранција за квалитетно и навремено извршување на договорот.

Банкарската гаранција за квалитетно и навремено извршување на договорот треба да биде во висина од 10% од вкупната вредност на договорот со пресметан данок на додадена вредност.

Гаранцијата се доставува во вид на банкарска гаранција во писмена форма или во електронска форма доколку е издадена како таква од банката во изворно оригинална форма. Гаранцијата треба да биде поднесена во оригинална форма. Копии не се прифаќаат.

Гаранцијата за квалитетно и навремено извршување на договорот треба да биде со важност до целосното реализирање на договорот.

Банкарската гаранција за квалитетно и навремено извршување на договорот треба да биде во валутата на која гласи договорот.

Со гаранцијата избраниот носителот на набавката гарантира дека предметот на договорот ќе го изврши на начинот и според динамиката предвидени во тендерската документација, односно техничката спецификација, доставената понуда и склучениот договор со договорниот орган.

Гаранцијата за квалитетно и навремено извршување на договорот ќе биде наплатена доколку носителот на набавката не исполни некоја од обврските од договорот за јавна набавка во рокот на стасаноста, за што писмено ќе го извести носителот на набавката.

Доколку договорот за јавна набавка е целосно реализиран согласно договореното, банкарската гаранција за квалитетно извршување на договорот договорниот орган му ја враќа на носителот на набавката во рок од 14 дена од целосното реализирање на договорот.

Гаранцијата за квалитетно и навремено извршување на договорот договорниот орган му ја враќа на носителот на набавката по пошта, лично во седиштето на економскиот оператор или лично во седиштето на договорниот орган.

Договорниот орган ќе ја наплати гаранцијата за квалитетно и навремено извршување на договорот и доколку дојде до негово едностране раскинување поради неизвршување на обврските од договорот од страна на носителот на набавката.

Договорниот орган нема да бара активирање на банкарската гаранција за квалитетно извршување на договорот од банката која ја има издадено доколку носителот на набавката поради непредвидени околности (виша сила или други оправдани причини) не можел да ја изврши набавката што е предмет на овој договор, во кој случај носителот на набавката треба да достави писмено образложение до договорниот орган во кое ќе ги наведе причините за неизвршување или ненавремено извршување на набавката, а кое треба да биде писмено прифатено од договорниот орган.

X. ДОВЕРЛИВОСТ НА ПОДАТОЦИ И ИНФОРМАЦИИ

Член 11

Определените лица од носителот на набавката наведени во понудата за реализација на договорот, задолжително потпишуваат изјава за доверливост на информации и податоци непосредно пред извршувањето на услугата - предмет на договорот.

Под поимот информации и податоци се подразбираат сите внатрешни и надворешни документи, спецификации, лични податоци, истражувања на пазарот или податоци за него, финансиски или маркетиншки информации, други податоци или бизнис, оперативни или технички информации, како и сите останати податоци и информации и независно дали се дадени во писмена, вербална или електронска форма и се во сопственост на договорниот орган.

Исто така, поимот информации и податоци, ги опфаќа и сите други податоци кои не се сопственост на договорниот орган, а се користат за одредени цели во работните задачи и обврски. Тука спаѓаат податоци на сите партнери, клиенти, добавувачи или било кое правно или физичко лице кое со Договорниот орган има засновано деловен или било каков друг однос. Договорниот орган ги става податоците на располагање на носителот на набавката во врска со погоре наведената цел, а за непречено одвивање на работните задачи и обврски.

Член 12

Не се предмет на овој договор информации кои биле или станале јавно достапни, но не како резултат на откривање од страна на носителот на набавката и на договорниот орган и без да бидат прекршени одредбите на овој договор од страна

на носителот на набавката што може да се докаже со писмена документација или за кои договорниот орган писмено потврдил дека се ослободени од обврска за неоткривање.

Член 13

Носителот на набавката под целосна морална, материјална и кривична одговорност, се обврзува за време на важноста на договорот и во период од (5) пет години од датумот на неговото истекување или раскинување да ги чува во тајност сите информации и податоци од било која област на договорниот орган, кои ќе му бидат дадени во процесот на соработката и притоа нема да ги искористи истите за лични цели, во име на друго лице, ниту ќе ги даде на увид на трета страна.

Носителот на набавката се обврзува да ги чува во тајност сите документи и податоци кои содржат информации за договорниот орган или неговите активности, како и неговите односи со клиенти или трети лица, а кои биле подготвени или изнесени во врска со работата за која Носителот на набавката е ангажиран од страна на договорниот орган.

Член 14

Носителот на набавката може да ги открие кои било од информациите и податоците наведени во членот 11 став 2 и 3 заради постапување по писмено барање од страна на надлежен орган, со легитимна наредба врз основа на закон.

Носителот на набавката, пред да ги даде бараните податоци ќе се увери дека барањето е валидно и е во согласност со важечки закон и ќе ги открие ваквите податоци само до степен до кој тоа е барано од надлежниот орган кој има овластување да бара такво соопштување.

Член 15

За секој настан или сомневање во однос на закана за нарушување на доверливоста, интегритетот и расположливоста на податоците и информациите, носителот на набавката се обврзува веднаш писмено да го извести определеното лице кај договорниот органот.

Член 16

Носителот на набавката по писмено барање на договорниот орган веднаш ќе ги врати или уништи сите документи кои содржат податоци и информации за договорниот орган, а кои се добиени во врска со работата за која носителот на набавката е ангажиран од страна на договорниот орган, без задржување на било какви фотокопии, изводи или друг вид на копии од нив или дел од нив. И покрај уништувањето на било кој податок и материјали носителот на набавката ќе продолжи да се придржува кон неговата обврска од овој договор и други обврски кои произлегуваат од него, за чување во тајност на сите податоци и информации

кои ги сознал на било кој начин, при исполнување на неговите обврски кои произлегуваат од овој договор.

Член 17

Објавувањето податоци, рекламирањето или публицитетот, како и прес конференциите направени од страна на Носителот на набавката во однос на овој договор или вршење на заеднички деловни активности на договорните страни треба да бидат претходно одобрени од договорниот орган пред нивното спроведување.

Член 18

Одредбите од глава X од овој договор се правно валидни и обврзувачки и кај сите вработени кај носителот на набавката кои имаат добиено овластување за користење на информациите и податоците кои се уредени со овој договор.

XI. УСЛОВИ ЗА РАСКИНУВАЊЕ ИЛИ ПРЕКИНУВАЊЕ ИЛИ НА ДОГОВОРОТ

Член 19

Овој договор може да се раскине спогодбено со согласност на двете договорни страни.

Член 20

Овој договор може да се раскине и едностране поради непридржување или неисполнување на договорните обврски утврдени со овој договор, како и поради неквалитетно вршење на работите утврдени со Договорот.

Договорната страна која поради непридржување или неисполнување на договорните обврски го раскинува договорот, должна е тоа да и го соопшти на другата договорна страна без одлагање во писмена форма.

Договорот се смета за раскинат со денот на приемот на известувањето за раскинување на договорот.

Доколку дојде до раскинување на договорот поради неисполнување или ненавремено исполнување на обврските на договорот од страна на носителот на набавката, покрај наплатата на банкарската гаранција, ќе биде одговорен за евентуалната штета што би ја предизвикал на договорниот орган како директна или индиректна последица на неговото работење.

Член 21

Кога една од договорните страни нема да ја исполни својата обврска, другата договорна страна може да бара исполнување на обврската од другата договорна страна или да го раскине договорот, а во секој случај има право на надомест на штетата од договорната страна која не ги исполнила своите обврски од договорот.

Член 22

Кога носителот на набавката нема да ја исполни својата обврска во определениот рок, договорниот орган може да и остави примерен дополнителен рок за исполнување на обврската.

Рокот од став 1 на овој член може да биде продолжен само по писмено барање на носителот на набавката и писмена согласност на договорниот орган.

Ако договорната страна која не ја исполнила својата обврска во рокот утврден со овој договор или не ја исполни обврската ни во дополнителниот рок, другата договорна страна може едностранo да го раскине договорот.

Доколку дојде до едностранo раскинување на договорот поради неисполнување на обврските од Договорот од страна на носителот на набавката, покрај наплатувањето на банкарската гаранција за квалитетно и навремено извршување на договорот, носителот на набавката ќе биде одговорен за евентуалната штета што би ја предизвикал на договорниот орган како директна или индиректна последица на неговото работење.

Член 23

Ниту една од договорните страни нема да биде одговорна за неисполнување на обврските од овој договор заради виша сила.

Под виша сила се подразбираат настани или околности на кои договорните страни не можат да влијаат и се надвор од нивната контрола, а го попречуваат нормалното извршување на договорот (елементарни непогоди, воени дејства, граѓански немири, штрајкови, и сл.).

Вишата сила не вклучува настан што е предизвикан од небрежност или намерна активност што би предизвикала застој во извршувањето на обврските од договорот.

Ако една од договорните страни е спречена да ги исполнува своите обврски заради виша сила, должна е веднаш писмено да ја извести другата страна, со наведување на причините за вишата сила и по можност обезбедување на соодветен доказ.

За времетраењето на вишата сила сите права и обврски од овој договор мируваат.

Договорните страни се обврзуваат на ист начин да ја известат договорната страна за повторното воспоставување на нормални услови за извршување на договорот, односно за престанокот на дејството на вишата сила.

По отстранувањето на вишата сила договорот продолжува да се реализира.

- Сектор за правни работи -

XII. ОПШТИ И ЗАВРШНИ ОДРЕДБИ

Член 24

Договорните страни можат да ги дополнат и/или изменат одредбите од овој договор само спогодбено.

Договорната страна која бара измена и/или дополнување е должна своето барање до другата страна да го достави во писмена форма.

Одредбите од овој договор можат да се изменат и/или дополнат со склучување анекс на договорот во согласност со Законот за јавните набавки.

Дополнувањата и измените на овој договор се важечки ако се направени во писмена форма и ако се потпишани од двете договорни страни.

За сé што не е предвидено со овој договор, се применуваат одредбите од Законот за облигационите односи, Законот за јавните набавки и другите позитивни законски прописи.

Член 25

Сите евентуални спорови кои би произлегле од овој договор, а кои договорните страни не би можеле да ги решат спогодбено, ќе ги решава надлежниот суд во Скопје.

Член 26

При секоја обработка на личните податоци во текот на реализацијата на овој договор, соодветно ќе се применуваат одредбите од Законот за заштита на личните податоци.

Член 27

Овој договор е составен во 4 (четири) еднообразни примероци од кои 2 (два) примерока за договорниот орган и 2 (два) примерока за носителот на набавката.

Договорен орган:
Република Северна Македонија
Министерство за финансии
Скопје

Dr. Fatmir Besimi
Министер за финансии

Носител на набавката:
Друштво за професионални и консултантски услуги ТЕЛЕЛИНК БИЗНИС СЕРВИСИС ДООЕЛ Скопје

Боби Цветковски
Управител

Изработил: Рената Николоска
Контролирал: Даниела Јанкова
Елизабета Калачоска
Одобрил: Татјана Васева
Проверил: Daut Hajrullahi
м-р Маја Стаменковска Угриновска
Согласен: д-р Јелена Таст

ПРИЛОГ 1 КОН ДОГОВОРОТ

ТЕХНИЧКИ СПЕЦИФИКАЦИИ

„Како дел од проектот потребно е да се достави претплата за 10-25 администратори за 12 месеци и да се обезбедат не помалку од следните функционалности (сите функционалности мора да бидат обезбедени од истиот производител):

- управување со корисници и привилегиран пристап (детален опис на барањата е вклучен во точка 1
- заштита од далечински пристап (детален опис на барањата може да се најде во 3)
- мулти-факторска автентикација и обезбедување пристап до клучните апликации преку порталот Single Sign-On (детален опис на барањата е вклучен во 2) "

Привилегирани корисници и управување со пристап

1. Системот мора да обезбеди функции за управување (автоматска промена на лозинка и дефинирање политика за пристап) со привилегирани корисници во:
   а) Оперативни системи: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390), Straus VOS
   б) Бази на податоци: Microsoft SQL, Microsoft SQL Cluster Service, Oracle, Informix, MySQL, Sybase Adaptive Server Enterprise, HeidiSQL, DB2, Informatica, MariaBD, MongoDB, PostgreSQL
   в) Системи и апликации за управување со инфраструктурата: DELL DRAC, IBM Tivoli, RSA менаџер за автентикација, HP iLO, SAP Application Server
   г) Мрежни уреди и безбедносни уреди: Cisco (рутери, nexus свичеви, заштитен ѕид), HP, Checkpoint, Netscreen, F5, Infoblox NIOS, FireEye Analware Malware, FortiGate, Aruba, Palo Alto Networks, A10, Riverbed, Gemalto
   д) CI/CD алатки: Chef, Jenkins, Kubernetes, Docker
   ѓ) SaaS апликации, веб-интерфејси, минимум: Facebook (на пр., маркетинг корисници), веб-услуги на Amazon (API и привилегирани корисници вклучувајќи root), Microsoft Azure (API и привилегирани корисници)
   е) Модули: Услуги на Microsoft, закажани задачи, базен на апликации IIS, безбедност на директориумот IIS, Регистрирај се, COM+, управување со корисници на домен на Microsoft
   ж) Лозинки зачувани во конфигурациски датотеки, табели со бази на податоци

з) Околини за виртуелизација VMWare ESX/ESXi"

2. Системот мора да обезбеди поддршка (заштита на корисничкиот профил и автоматско ротирање на лозинката) за кој било уред што поддржува ODBC верзија 2.7 или повисока
3. Системот мора да обезбеди поддршка (способност за управување со привилегирани корисници што се користат во целниот систем) за системи надвор од списокот „out-of-the box" користејќи скрипти или други механизми имплементирани и поддржани од производителот на решението, достапни бесплатно на официјалната веб-страница на производителот на растворот. Не помалку од 200 уникатни интеграции ќе бидат достапни во рамките на порталот.
4. Системот мора да поддржува заштита на локални администраторски корисници и автоматско ротирање на лозинките на работни станици на Windows и MAC OS (Заштита на системите кои често се надвор од локалната мрежа). Системот мора да обезбеди алатка/агент инсталиран на работната станица, кој ќе се интегрира со предложеното решение (под истата лиценца) за промена на лозинката на работната станица (кога станицата е поврзана на локалната мрежа) и ќе го информира системот за завршување на промената задача.
5. Системот мора да обезбеди поддршка (способност за управување со привилегирани сметки што се користат во целниот систем) за апликации надвор од списокот „ out-of-the box " со помош на скрипти или други механизми имплементирани и поддржани од производителот на решението за промена и верификација на лозинки преку: SSH / Телнет , API за надворешни апликации , симулација на кориснички дејства во сесија на веб-апликација.
6. Системот мора да обезбеди можност за автоматско откривање корисници во нови уреди со Windows, услуги на Windows, закажани задачи, корисници за услуги на IIS итн., исто така, автоматски вградени откриени корисници и автоматски да ја спроведува соодветната политика за управување со привилегираниот корисник.
7. Системот мора да има способност да заштити (управува) и динамички да генерира нови SSH клучеви според наведениот шаблон
8. Системот мора да ја потврди лозинката / клучот SSH зачуван во предложеното решение со лозинката / клучот SSH зачуван на целниот систем според дефинираната политика
9. Системот мора да ја усогласи лозинката / клучот SSH зачуван во предложеното решение со лозинката / клучот SSH зачуван на целниот систем во случај на недоследност
10. Системот мора да ја зачува историјата на лозинки (на пр. три најнови верзии) и да обезбеди лесен пристап до историјата (на пр. преку веб-интерфејс)
11. Системот мора да поддржува различни LDAP средини, минимум: Sun One, MS Active-Directory, IBM Tivoli, Novel eDirectory, Oracle Internet Directory

12. Системот мора да обезбеди SSH откривање на парови на клучеви во инфраструктурата
13. Системот мора да обезбеди управување со SSH клучеви и безбедност на клучевите SSH што ги користат апликациите во конфигурациските датотеки
14. Добавувачот мора да обезбеди бесплатна апликација која се користи за автоматизирање на процесот на креирање нови скрипти одговорни за ротирање на ингеренциите со SSH протокол. Апликацијата мора да може да го сними процесот на најавување на корисникот и ротација на ингеренциите во целниот систем, а потоа врз основа на снимањето мора автоматски да генерира скрипта/приклучок што ќе го користи моторот за автоматско управување со ингеренциите на сметката.

Привилегирано управување со сесиите

15. креирање нови скрипти одговорни за ротирање на ингеренциите со SSH протокол. Апликацијата мора да може да го сними процесот на најавување на корисникот и ротација на ингеренциите во целниот систем, а потоа врз основа на снимањето мора автоматски да генерира скрипта/приклучок што ќе го користи моторот за автоматско управување со ингеренциите на сметката.
16. Системот мора да поддржува изолација и следење на сесиите без потреба да се открие лозинката / клучот ssh на привилегираниот корисник на корисничката станица. Кога крајниот корисник е безбедно автентициран на Модулот за раздвојување на системот и е наведен привилегираниот корисник, предложеното решение мора автоматски да ги преземе привилегираните ингеренции од централниот репозиториум, да ја стартува апликацијата избрана претходно од корисникот (апликацијата е инсталирана на модулот за одвојување) и автоматски да ги внесе ингеренциите во апликацијата (да не се дистрибуираат на корисничката работна станица). Снимањето сесии со индексирање на податоци мора да биде достапно како опција во дефинирањето на политиките. Во случај на управување со врските на веб-прелистувачот преку системот за одделување модули, мора да го зацврсти веб-прелистувачот (на пр., да го оневозможи менито за адреси, алатките, да го блокира внесувањето на корисникот за време на процесот на вбризгување акредитиви итн.
17. Системот мора да поддржува изолација и следење на сесиите без потреба да се открие лозинката / клучот ssh на привилегираниот корисник на корисничката станица. Кога крајниот корисник е безбедно автентициран на Модулот за раздвојување на системот и е наведен привилегираниот корисник, предложеното решение мора автоматски да ги преземе привилегираните ингеренции од централниот репозиториум, да ја стартува апликацијата избрана претходно од

корисникот (апликацијата е инсталирана на модулот за одвојување) и автоматски да внесе ингеренциите во апликацијата (да не се дистрибуираат на корисничката работна станица). Снимањето сесии со „Системот мора безбедно да воспостави и да управува со привилегирани сесии за не помалку од следниве системи:

а) Оперативни системи: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390)

б) Бази на податоци: Microsoft SQL, Oracle, MySQL, SAP HANA, HeidiSQL, DB2

в) Системи и апликации за управување со инфраструктурата: DELL DRAC, RSA менаџер за автентикација, HP iLO, SAP GUI, BMC Remedy

г) Мрежни уреди и безбедносни уреди: Cisco (рутери, nexus свичеви, заштитен sид), HP, Checkpoint (SmartDashboard, https, ssh), Radware, F5 Networks, FortiGate, Palo Alto Networks

д) Алатки за CI/CD (https, ssh): готвач, Џенкинс, Кубернетс, Докер, Jfrog, GitHub

ѓ) Веб-услуги: SaaS услуги, веб-интерфејси, минимум: Facebook (на пр. маркетинг сметки), веб-услуги на Amazon (управувачка конзола, IAM, STS интеграција), управување со Microsoft Azure

е) Околини за виртуелизација: VMWare ESX/ESXi, vCenter (vSphere Client, https, ssh)

18. Модулот за прокси мора да ја поддржува функционалноста на Microsoft Remote App за објавување апликации. Скриптите за стврднување мора да бидат испорачани од продавачот на PAM и да се извршат за време на инсталацијата на производот.
19. „Системот мора да обезбеди кориснички пристап до заштитениот ресурс со не помалку од следните алатки/методи:

а) Веб интерфејс на привилегирано безбедносно решение за акаунтот

б) Различни клиенти/менаџери на RDP што се користат на станицата од која се врши привилегиран пристап со не помалку од: дефинирање параметри за поврзување во конфигурациската датотека на клиентот RDP или интерактивно барање корисник за својствата на заштитениот систем (како што се адреса, апликација на клиент, привилегирана сметка име). Системот мора да поддржува PKI сертификати како метод за директно автентикација на Separation Module.

в) Веб-прелистувач кој поддржува html5 за да обезбеди безбеден кориснички пристап за оперативни системи различни од Windows (без клиент RDP). Привилегираната сесија (мора да биде тунелирана во html5 и достапна за корисникот како нова картичка во прелистувачот.

г) Различни командна линија и SSH клиенти (на пр. кит), со автентикација на системот заснована на клучеви SSH."

20. Системот мора да обезбеди опција за крајниот корисник да избере дали конкретната графичка сесија треба да се воспостави со протокол RDP или HTTPS (сесија тунелирана во HTML5)
21. Системот мора да обезбеди временски ограничен привилегиран пристап со привремено доделување акаунт на Windows (локален или домен) на група локални администратори по поднесување соодветно барање (Пристап само на време). Дозволите доделени од Системот мора автоматски да се деактивираат по надминување на одобрената временска рамка за подигање на привилегиите.
22. По повеќефакторската автентикација на системот за графички интерфејс мора да обезбеди функционалност за генерирање и преземање приватен SSH клуч (системот мора да обезбеди полиса за декларација за време на важност на клучот) за да се овозможи безбеден пристап до целните средства преку прокси-модулот без потреба да се обезбедат дополнителни фактори за автентикација. Мора да се обезбеди пристап до целните системи врз основа на RBAC доделен на корисникот кој го генерирал и преземал SSH. Системот мора да обезбеди заштита на лозинка за генерирани SSH клучеви со дефинирана должина и сложеност на лозинката.

Управување со безбедносни инциденти

23. Системот мора да обезбеди категоризација на снимените кориснички сесии со претходно дефинирани нивоа на ризик. Ризикот мора да се дефинира врз основа на збир на политики на функции/команди откриени за време на сесијата и тежината што им е доделена. Ризикот мора автоматски да се анализира за време на тековните сесии. Информациите за нивото на ризик доделено на сесијата мора да бидат видливи и во конзолата за следење на сесиите и во интерфејсот на контролната табла за безбедносни инциденти. Администраторот мора да може да одреди кои дејства што ги врши корисникот треба автоматски да бидат суспендирани или прекинати.
24. Системот мора да има вградени аналитички алатки кои овозможуваат автоматско (без барање за рачно дефинирање правила за безбедносна политика) откривање на сомнителни активности на привилегирани корисници. Откривањето мора да се потпира на автоматски научено однесување на поединечни корисници (стандардно работно време, опсег на IP адреса, количина на референци до складиштето на профилот за преземање лозинки).
25. Системот треба да собира и анализира податоци за активноста на корисникот од надворешни SIEM системи, не помалку од следниве решенија мора да бидат поддржани: Arcsight, Qradar, Splunk, LogRhythm, RSA, McAfee и оперативни системи: rsyslog (од Unix / Linux системи), Windows Event Препраќач (од Windows системи), AWS CloudTrail, апликација Azure Function.

26. Системот мора да има опција за поправка и извршување на дејството за одговор (барем принудувајќи ја да се смени лозинката за привилегираниот кориснички профил) ако се открие сомнително користење на привилегираниот акаунт (кражба на акредитиви на привилегираниот акаунт или создавање нов привилегиран акаунт).
27. Системот мора да генерира соодветен аларм во случај на откривање прекумерно користење на привилегирани акаунти и во случај на користење на привилегираниот акаунт во нестандардни часови (на пр. надвор од работното време типично за даден корисник)
28. Системот треба да открие инцидент кога привилегираните ингеренции се користат за директно поврзување со целниот систем (без добивање лозинка од заштитеното складиште) и настан кога се креира нов привилегиран акаунт во системот. За безбедносните настани опишани во оваа точка системот мора да обезбеди процедури за автоматска санација, не помалку од: ресетирање на лозинка за привилегираниот акаунт кога ќе се случи безбедносен инцидент, автоматско (неуправувано) вклучување на акаунтот и автоматско усогласување на лозинките.
29. Системот мора да може да детектира нови неуправувани привилегирани профили и врски низ AWS и Azure околината што биле воспоставени без да ја преземе лозинката од централното складиште.
30. Системот мора да обезбеди функционалности на ревизорот за: следење на тековната сесија, суспендирање / прекинување на сесиите, дефинирање група настани (наредби, стартување апликација итн.) за кои системот автоматски треба да ја заврши / суспендира сесијата (функцијата за завршување / суспендирање на сесијата мора да биде достапна барем за внатрешни претплата / лиценца за вработени)

Архитектура

31. Системот мора да обезбеди опција за инсталирање на базата на податоци на централно складиште за акредитиви на одвоен, зацврстен оперативен систем што нема да биде споделен со други модули, како што се нас: прокси за изолација на сесија, веб-интерфејс, аналитички модул, мотор за ротација на лозинка.
32. Целото решение мора да биде обезбедено од истиот производител, поединечните функционални модули мора да се интегрираат едни со други
33. Системот мора да биде модуларен, со компоненти за проширување достапни под посебни претплати / лиценци, за не помалку од:

- мултифакторска автентикација и управување со пристап до веб-апликации и безбедност (за внатрешни и апликации базирани на облак) со доставување на функционалност за еднократно пријавување
- заштита од далечински пристап за вработените и надворешните добавувачи, барања
- интеграција со надворешни комерцијални системи како IAM, RPA, алатки за ранливост,
- Спроведување на најмала привилегија врз основа на агенти на станиците на Windows со бришење локални администраторски сметки и зголемување на правата во контекст на специфични објекти (скрипти, апликации, инсталации, dll и друго) за одредени корисници, контрола на апликации и блокирање на протекување на ингеренциите (на пр. лозинки) од складишта и апликации на оперативниот систем Windows (на пр. веб-прелистувачи, LSASS меморија, SAM и други),
- заштита на тајните во средини DevOps
- заштита на привилегирани сметки вградени во статични апликации и административни скрипти
- управување со правата во Cloud платформи
- Спроведување на најмала привилегија базирано на агенти на серверите Linux / Unix (централно управување со дозволеното / недозволено извршување команда, централно покачување на привилегијата, корисничка одговорност, снимање на локална сесија), барања
- модул кој овозможува складирање на ингеренциите на деловните корисници во складиштето за лозинки

34. Добавувачот на PAM мора да обезбеди процедури кои го опишуваат методот на подобрување на секоја од компонентите на системот и да обезбеди скрипти кои го автоматизираат процесот на зацврстување на безбедноста во инсталационите пакети, приспособени на секој од функционалните модули. Подобрувањето на секоја од компонентите мора да се изврши во согласност со најдобрите практики на производителот на оперативниот систем и производителот на растворот PAM/PAS. Подобрувањето на оперативниот систем на складиштето за акредитиви мора да се изврши автоматски од страна на инсталерот за време на процесот на инсталација на модулот.
35. Системот треба да вклучува не помалку од: еден модул за складиште за лозинки, 5x модул за складиште за целите на враќање од катастрофи / висока достапност, 5x модул за промени и управување со клучеви и лозинки во заштитените системи, 2 тест околини што овозможуваат мапирање на производната средина.

36. Решението не може да го ограничи бројот на модули што се користат за изолација на сесиите на следење, како и веб-кориснички интерфејси на решението (додавањето дополнителни модули нема да бара купување дополнителни лиценци / претплати од Добавувачот на системот PAM).
37. Системот мора да поддржува дистрибуирана архитектура, во која поединечни функционални модули (прокси-прокси, модули за тајно ротирање, интерфејси WebUI) се инсталирани на повеќе локации (географски одвоени) и комуницираат со централните елементи (складиште за акредитиви) користејќи безбеден протокол за комуникација (обезбедување податоци безбедност за време на преносот, работи преку една TCP порта, која може да се декларира при инсталирање на системот). Во случај на дистрибуирана инфраструктура, целиот систем мора да се управува од централен графички интерфејс.
38. Високата достапност на модулот за складирање привилегирани сметки мора да се имплементира на слојот на предложениот софтвер (апликација), а не на оперативниот систем / базата на податоци на кој е инсталиран софтверот
39. Производот мора да обезбеди криптографска заштита за резервните копии генерирани од производот
40. Решението мора да обезбеди функционалност за имплементирање на модулите за складирање на привилегирани сметки во дистрибуирана форма, заснована на: активен модул, вишок на активниот модул и збир на активни географски распределени модули, обезбедувајќи (во режим на читање) најкритични функции за крајните корисници. (на пр. механизми за резервна копија, споделување податоци за привилегирани сметки со апликации, пристап до корисничкиот интерфејс, воспоставување привилегирани сесии на безбеден начин). Предложеното решение мора да поддржува не помалку од 6 активни складишта за акредитиви. Во случај на дистрибуирана инфраструктура, целиот систем мора да се управува од централен графички интерфејс.
41. Репозиториумот во кој се чуваат заштитени привилегирани акаунти мора да се доставува со резервни компоненти за враќање од катастрофи на географски одвоени локации. Мора да биде можно да се користат не помалку од следниве методи за висока достапност и враќање при катастрофи:

    а) режимот на висока достапност помеѓу два тајни системи на складиште кои го делат просторот на дискот со шифрирана база на податоци

    б) модули за враќање од катастрофи на други локации (мора да биде можно да се имплементираат до 4 модули за враќање од катастрофи како дел од основната претплата со распоредениот НА на примарната локација)

    Мора да биде возможно да се имплементираат двата опишани методи (а и б) во иста производна средина".

42. Решението мора да обезбеди "breaking glass offline" пристап до привилегирани тајни во посветена мобилна апликација (достапна на оперативните системи IOS и Android). Системскиот администратор мора да може да дефинира ситуации во кои ќе се активира офлајн пристапот, не помалку отколку за следните сценарија: не е достапна мрежна врска од мобилната апликација, кога услугата за пристап не е достапна, администраторот мора да може да одреди дали офлајн пристапот е достапни само за корисници на компанијата или, исто така, продавачи од трета страна.

Интеграција

43. Системот мора да обезбеди можност за интегрирање со SIEM решенијата за испраќање информации за регистрирани настани како дел од набљудуваните сесии. Системот мора да обезбеди можност да конфигурира какви видови настани треба да се испраќаат до системот SIEM.
44. Системот мора да обезбеди интеграција со системите за отврање на инциденти, не помалку од: BMC Remedy, ServiceNow и друго преку отворено API, сфатено како потврда дали постои точен инцидент во системот за инциденти и дали има соодветен статус за да може да се дозволи пристап за примање привилегирани ингеренциите или воспоставете привилегирана врска.
45. Системот мора да обезбеди интеграција со HSM-уреди базирани на PKCS#11, не помалку од: Atos HSM Proteccio, Gemalto Luna/Safenet 1700 Хардверски безбедносен модул, Thales nShield Хардверски безбедносен модул, Utimaco CryptoServer, Crypto4A QxEDGE, Fortanix Unident TSDK Контрола, Utimaco CryptoServer.
46. Системот обезбедува интеграција со голем број методи за автентикација, не само лозинки, LDAP, Windows NTLM, SSH клучеви, паметни картички, PKI, RADIUS, SAML, MFA, RSA SecurID, Oracle SSO, Amazon Cognito Authentication, OpenID Connect (OIDC)

Дополнителни карактеристики и функционалности

47. Официјалната методологија за имплементација треба да биде достапна на веб-страницата на производителот. Оваа методологија мора да го опфати описот на главните чекори што треба да се преземат за правилно и сеопфатно имплементирање на PAS решение со: заштита на привилегиран пристап, спроведување политика на најмалку привилегии за работни станици и сервери и заштита на привилегирани акаунти и тајни што ги користат апликациите за

пристап до други целни системи (вклучувајќи заштита на средини управувани од DevOps). Клучните привилегирани типови сметки треба да се класифицираат и да се засноваат на анализа на ризик. Методологијата мора да биде достапна на официјалната веб-страница на производителот, а кон понудата треба да се приложи линк до официјалната веб-страница на производителот што содржи опис на методологијата.

48. Предложеното решение треба да се наоѓа во квадрантот „Лидери“ од извештајот Gartner Magic Quadrant for Privileged Access Management.
49. Системот треба да обезбеди централно управување со политиките (централна дефиниција на бели листи/црни листи на команди со параметри, доделени на привилегирани сметки и групи луѓе) за мрежен и локален привилегиран пристап за Linux/Unix сервери.
50. Системот треба да обезбеди SUDO централизирана функционалност за замена
51. Системот треба да обезбеди снимање на локални сесии и кориснички команди. Кога сесијата ќе заврши, снимките треба да се складираат на безбеден шифриран начин во централното складиште.
52. Системот треба да обезбеди функционалност за спроведување на управувањето со командите со нивните дополнителни параметри и доделување политика на групите
53. Системот треба да ги заштити логовите од отстранување/модификации.
54. Системот треба да спречи т.н. shell escape (корисниците не можат да извршат ограничена команда од друга програма, на пример: извршете ограничена команда од уредувачот vi отворен со зголемени права).
55. Системот треба да обезбеди опција за интегриран Unix/Linux сервер со AD околина со вградена функционалност AD Bridge (OPM PAM).
56. Системот мора да обезбеди интеграција помеѓу безбедносниот модул за идентитет и складиштето за лозинки за безбедно складирање на тајните на деловните корисници и автоматски да ги вбризга преку приклучок во прелистувачот на корисникот на веб-апликации достапни на порталот SSO (Single sign on)
57. Системот мора автоматски да ги препознава посетите на нови деловни веб-локации каде од корисникот ќе биде побарано автентикација. Ингеренциите обезбедени од корисникот мора да се фатат и да се зачуваат во складиштето за лозинки и соодветната нова веб-апликација мора да се додаде во каталогот на апликации на порталот SSO (Single sign on).
58. Системот мора да го обезбеди приклучокот на корисничкиот прелистувач со вградена функција за генерирање лозинки. Генераторот на лозинки мора да дозволи да се специфицира најмалку должината на лозинката и сложеноста на новогенерираната лозинка (системот мора да дозволи да избере дали броевите, симболите, големите и малите букви треба да се користат во новогенерирана лозинка).

59. Системот мора да обезбеди дополнителна компонента (со дополнителна претплата, која не е вклучена во тековната фаза на проектот) како продолжување на модулот за SSO (Single sign on)што овозможува барем:

а) запишете ги сите кориснички активности користејќи "stepper" пристап, . Системот мора да активира слика од екранот на прозорецот на прелистувачот на корисникот заедно со релевантните метаподатоци за барем следните дејства што ги прави корисникот за време на набљудуваната веб-сесија: кликнувања на глувчето, притискање на тастатурата „enter" или „tab". Системот мора да дозволи да се пребаруваат сите снимени сесии користејќи бесплатно внесување текст и да ги филтрира безбедносните настани по датуми и дејства.

б) идентификувајте кога сесијата со висок ризик е оставена отворена и бара повторна автентикација за да се осигура дека лицето кое ја иницирало веб-сесијата е овластено,

в) заштита на веб-сесијата на крајната точка со екстензијата на прелистувачот

Прилог 1

ОБРАЗЕЦ НА ПОНУДА

Bobi Cvetkovski

Digitally signed by Bobi Cvetkovski
Date: 2022.10.31 11:57:51 +01'00'

Врз основа на оглас 17338/2022 објавен од страна на Министерството за финансии, за доделување на договор за јавна набавка на стоки – управување со привилегиран пристап (PAM), со спроведување на поедноставена отворена постапка преку Електронскиот систем за јавни набавки (https://www.e-nabavki.gov.mk) и на тендерската документација ја поднесуваме следнава:

П О Н У Д А

Дел I – Информации за понудувачот

I.1. Име на понудувачот: Телелинк Бизнис Сервисис Дооел

I.2. Контакт информации:

-Адреса: Фјодор Достоевски бр. 72, вл.1 кат 4/ стан 5, 1000 Скопје

-Телефон: +38970363730

-Факс: +38923073521

-Е-пошта: bobi.cvetkovski@tbs.tech

-Лице за контакт: Боби Цветковски

I.3. Одговорно лице: Боби Цветковски

I.4. Даночен број: 4057019547562

I.5. Матичен број на понудувачот: 7385986

I.6. Согласни сме да ја дадеме оваа понуда за предметот на договорот за јавна набавка согласно со техничките спецификации.

Дел II – ТЕХНИЧКА ПОНУДА

II.1. Согласни сме да ви го обезбедиме предметот на набавка – управување со привелигиран пристап (PAM): **CyberArk Privileged Access Management** (да се наведе називот на понудениот систем), сметано од денот на целосната инсталација и ставање во употреба на истиот во се според барањата дефинирани во техничките спецификации кои се составен дел од тендерската документација.

*** Називот на понуденото решение и описот што обезбедува системот задолжително се потполнува, во спротивно понудата ќе биде отфрлена како неприфатлива.**

II.2. Во прилог на техничката понуда да се достави технички опис како ќе се постигнат следните карактеристики барани за управување со привилегиран пристап (PAM).

Карактеристики се бараат да ги обезбеди системот	**Опис што обезбедува системот**
Привилегирани корисници и управување со пристап	
Системот мора да обезбеди функции за управување (автоматска промена на лозинка и дефинирање политика за пристап) со привилегирани корисници во: а) Оперативни системи: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390), Straus VOS б) Бази на податоци: Microsoft SQL, Microsoft SQL Cluster Service, Oracle, Informix, MySQL, Sybase Adaptive Server Enterprise, HeidiSQL, DB2, Informatica, MariaBD, MongoDB, PostgreSQL в) Системи и апликации за управување со инфраструктурата: DELL DRAC, IBM Tivoli, RSA менаџер за автентикација, HP iLO, SAP Application Server г) Мрежни уреди и безбедносни уреди: Cisco (рутери, nexus свичеви, заштитен ѕид), HP, Checkpoint, Netscreen, F5, Infoblox NIOS, FireEye Analware Malware, FortiGate, Aruba, Palo Alto Networks, A10, Riverbed, Gemalto	Системот обезбедува функции за управување (автоматска промена на лозинка и дефинирање политика за пристап) со привилегирани корисници во: а) Оперативни системи: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390), Straus VOS - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/PASIMP/Operating-Systems.htm б) Бази на податоци: Microsoft SQL, Microsoft SQL Cluster Service, Oracle, Informix, MySQL, Sybase Adaptive Server Enterprise, HeidiSQL, DB2, Informatica, MariaBD, MongoDB, PostgreSQL - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/PASIMP/Databases.htm в) Системи и апликации за управување со инфраструктурата: DELL DRAC, IBM Tivoli, RSA менаџер за автентикација, HP iLO, SAP Application Server - https://cyberark-customers.force.com/mplace/s/#---CyberArk_Solution__c-PrivilegedCredentialsManagement г) Мрежни уреди и безбедносни уреди: Cisco (рутери, nexus свичеви, заштитен ѕид), HP, Checkpoint, Netscreen, F5, Infoblox NIOS, FireEye Analware Malware, FortiGate, Aruba, Palo Alto Networks, A10, Riverbed, Gemalto –

д) CI/CD алатки: Chef, Jenkins, Kubernetes, Docker ѓ) SaaS апликации, веб-интерфејси, минимум: Facebook (на пр., маркетинг корисници), веб-услуги на Amazon (API и привилегирани корисници вклучувајќи root), Microsoft Azure (API и привилегирани корисници) е) Модули: Услуги на Microsoft, закажани задачи, базен на апликации IIS, безбедност на директориумот IIS, Регистрирај се, COM+, управување со корисници на домен на Microsoft ж) Лозинки зачувани во конфигурациски датотеки, табели со бази на податоци з) Околини за виртуелизација VMWare ESX/ESXi"	https://cyberark-customers.force.com/mplace/s/#---CyberArk_Solution__c-PrivilegedCredentialsManagement д) CI/CD алатки: Chef, Jenkins, Kubernetes, Docker – https://cyberark-customers.force.com/mplace/s/#a352J000000pq0gQAA-a392J000001h4e1QAA и https://cyberark-customers.force.com/mplace/s/#a3550000000EmdeAAC-a3950000000jkdVAAQ ѓ) SaaS апликации, веб-интерфејси, минимум: Facebook (на пр., маркетинг корисници), веб-услуги на Amazon (API и привилегирани корисници вклучувајќи root), Microsoft Azure (API и привилегирани корисници) – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Cloud-Services.htm?tocpath=Administrator%7CComponents%7CCentral%20Policy%20Manager%7CPM%20plugins%7CTarget%20account%20plugins%7CCloud%20services%7C___0 е) Модули: Услуги на Microsoft, закажани задачи, базен на апликации IIS, безбедност на директориумот IIS, Регистрирај се, COM+, управување со корисници на домен на Microsoft – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/Landing%20Pages/LPServicePlugins.htm?tocpath=Administrator%7CComponents%7CCentral%20Policy%20Manager%7CPM%20plugins%7CService%20account%20plugins%7C___0 ж) Лозинки зачувани во конфигурациски датотеки, табели со бази на податоци – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/AccountsStoredInConfigurationFiles.htm?tocpath=Administrator%7CComponents%7CCentral%20Policy%20Manager%7CPM%20plugins%7CService%20account%20plugins%7C___6 и https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/AccountsStoredInDatabases.htm?tocpath=Administrator%7CComponents%7CCentral%20Policy%20Manager%7CPM%20plugins%7CService%20account%20plugins%7C___7 з) Околини за виртуелизација VMWare ESX/ESXi"

	https://cyberark-customers.force.com/mplace/s/#a352J000000ptE8QAI-a392J000001h4zyQAA
Системот мора да обезбеди поддршка (заштита на корисничкиот профил и автоматско ротирање на лозинката) за кој било уред што поддржува ODBC верзија 2.7 или повисока	Системот обезбедува поддршка (заштита на корисничкиот профил и автоматско ротирање на лозинката) за кој било уред што поддржува ODBC верзија 2.7 или повисока - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/DatabasesthatSupportODBCConnectionsPlugin.htm
Системот мора да обезбеди поддршка (способност за управување со привилегирани корисници што се користат во целниот систем) за системи надвор од списокот „out-of-the box" користејќи скрипти или други механизми имплементирани и поддржани од производителот на решението, достапни бесплатно на официјалната веб-страница на производителот на растворот. Не помалку од 200 уникатни интеграции ќе бидат достапни во рамките на порталот	Системот обезбедува поддршка (способност за управување со привилегирани корисници што се користат во целниот систем) за системи надвор од списокот „out-of-the box" користејќи скрипти или други механизми имплементирани и поддржани од производителот на решението, достапни бесплатно на официјалната веб-страница на производителот на растворот. Не помалку од 200 уникатни интеграции ќе бидат достапни во рамките на порталот – https://cyberark-customers.force.com/mplace/s/#all
Системот мора да поддржува заштита на локални администраторски корисници и автоматско ротирање на лозинките на работни станици на Windows и MAC OS (Заштита на системите кои често се надвор од локалната мрежа). Системот мора да обезбеди алатка/агент инсталиран на работната станица, кој ќе се интегрира со предложеното решение (под истата лиценца) за промена на лозинката на работната станица (кога станицата е поврзана на локалната мрежа) и ќе го информира системот за завршување на промената задача.	Системот поддржува заштита на локални администраторски корисници и автоматско ротирање на лозинките на работни станици на Windows и MAC OS (Заштита на системите кои често се надвор од локалната мрежа). Системот обезбедува алатка/агент инсталиран на работната станица, кој ќе се интегрира со предложеното решение (под истата лиценца) за промена на лозинката на работната станица (кога станицата е поврзана на локалната мрежа) и ќе го информира системот за завршување на промената задача. – https://docs.cyberark.com/Product-Doc/OnlineHelp/EPM-onprem/Latest/en/Content/EPM_PET/Endpoint%20Machines%20Supported%20Operating%20Systems.htm
Системот мора да обезбеди поддршка (способност за управување со привилегирани сметки што се користат во	Системот мора да обезбеди поддршка (способност за управување со привилегирани сметки што се користат во целниот систем) за апликации надвор од списокот „ out-of-

целниот систем) за апликации надвор од списокот „ out-of-the box " со помош на скрипти или други механизми имплементирани и поддржани од производителот на решението за промена и верификација на лозинки преку: SSH / Телнет , API за надворешни апликации , симулација на кориснички дејства во сесија на веб-апликација.	the box " со помош на скрипти или други механизми имплементирани и поддржани од производителот на решението за промена и верификација на лозинки преку: SSH / Телнет , API за надворешни апликации , симулација на кориснички дејства во сесија на веб-апликација. - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Privileged-Session-Manager-SSH-Proxy-Introduction.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____0
Системот мора да обезбеди можност за автоматско откривање корисници во нови уреди со Windows, услуги на Windows, закажани задачи, корисници за услуги на IIS итн., исто така, автоматски вградени откриени корисници и автоматски да ја спроведува соодветната политика за управување со привилегираниот корисник.	Системот обезбедува можност за автоматско откривање корисници во нови уреди со Windows, услуги на Windows, закажани задачи, корисници за услуги на IIS итн., исто така, автоматски вградени откриени корисници и автоматски да ја спроведува соодветната политика за управување со привилегираниот корисник. – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/Landing%20Pages/LP ServicePlugins.htm?tocpath=Administrator%7CComponents%7CCentral%20Policy%20Manager%7CCPM%20plugins%7CService%20account%20plugins%7C____0 и https://www.cyberark.com/resources/product-datasheets/cyberark-dna-datasheet
Системот мора да има способност да заштити (управува) и динамички да генерира нови SSH клучеви според наведениот шаблон	Системот има способност да заштити (управува) и динамички да генерира нови SSH клучеви според наведениот шаблон – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PrivateSSHKey.htm?tocpath=Administrator%7CComponents%7CCentral%20Policy%20Manager%7CCPM%20plugins%7CService%20account%20plugins%7C____8 и https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Managing%20SSH%20Keys.htm
Системот мора да ја потврди лозинката / клучот SSH зачуван во предложеното решение со лозинката / клучот SSH зачуван на целниот систем според дефинираната политика	Системот ја потврдува лозинката / клучот SSH зачуван во предложеното решение со лозинката / клучот SSH зачуван на целниот систем според дефинираната политика – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Managing%20SSH%20Keys.htm

Системот мора да ја усогласи лозинката / клучот SSH зачуван во предложеното решение со лозинката / клучот SSH зачуван на целниот систем во случај на недоследност	Системот ја усогласува лозинката / клучот SSH зачуван во предложеното решение со лозинката / клучот SSH зачуван на целниот систем во случај на недоследност – Системот мора да ја усогласи лозинката / клучот SSH зачуван во предложеното решение со лозинката / клучот SSH зачуван на целниот систем во случај на недоследност – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Managing%20SSH%20Keys.htm
Системот мора да ја зачува историјата на лозинки (на пр. три најнови верзии) и да обезбеди лесен пристап до историјата (на пр. преку веб-интерфејс)	Системот ја зачувува историјата на лозинки (на пр. три најнови верзии) и да обезбеди лесен пристап до историјата (на пр. преку веб-интерфејс) – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Password-Version-Control.htm
Системот мора да поддржува различни LDAP средини, минимум: Sun One, MS Active-Directory, IBM Tivoli, Novel eDirectory, Oracle Internet Directory	Системот поддржува различни LDAP средини, минимум: Sun One, MS Active-Directory, IBM Tivoli, Novel eDirectory, Oracle Internet Directory – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Directories.htm?tocpath=Administrator%7CComponents%7CCentral%20Policy%20Manager%7CCPM%20plugins%7CTarget%20account%20plugins%7CDirectories%7C 0 и https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Plugins/plugin-LDAP.htm
Системот мора да обезбеди SSH откривање на парови на клучеви во инфраструктурата Системот мора да обезбеди управување со SSH клучеви и безбедност на клучевите SSH што ги користат апликациите во конфигурациските датотеки	Системот обезбедува SSH откривање на парови на клучеви во инфраструктурата Системот мора да обезбеди управување со SSH клучеви и безбедност на клучевите SSH што ги користат апликациите во конфигурациските датотеки – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Providing%20SSH%20Keys%20Lifecycle%20Management.htm?tocpath=Administrator%7CComponents%7CSSH%C2%A0Key%20Manager%7C 1

Добавувачот мора да обезбеди бесплатна апликација која се користи за автоматизирање на процесот на креирање нови скрипти одговорни за ротирање на ингеренциите со SSH протокол. Апликацијата мора да може да го сними процесот на најавување на корисникот и ротација на ингеренциите во целниот систем, а потоа врз основа на снимањето мора автоматски да генерира скрипта/приклучок што ќе го користи моторот за автоматско управување со ингеренциите на сметката.	Добавувачот обезбедува бесплатна апликација која се користи за автоматизирање на процесот на креирање нови скрипти одговорни за ротирање на ингеренциите со SSH протокол. Апликацијата го снима процесот на најавување на корисникот и ротација на ингеренциите во целниот систем, а потоа врз основа на снимањето мора автоматски да генерира скрипта/приклучок што ќе го користи моторот за автоматско управување со ингеренциите на сметката. - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Introduction.htm?tocpath=Administrator%7CComponents%7CSSH%C2%A0Key%20Manager%7C 0
Привилегирано управување со сесиите	
креирање нови скрипти одговорни за ротирање на ингеренциите со SSH протокол. Апликацијата мора да може да го сними процесот на најавување на корисникот и ротација на ингеренциите во целниот систем, а потоа врз основа на снимањето мора автоматски да генерира скрипта/приклучок што ќе го користи моторот за автоматско управување со ингеренциите на сметката.	Во системот може да се креираат нови скрипти одговорни за ротирање на ингеренциите со SSH протокол. Апликацијата може да го сними процесот на најавување на корисникот и ротација на ингеренциите во целниот систем, а потоа врз основа на снимањето автоматски да генерира скрипта/приклучок што ќе го користи моторот за автоматско управување со ингеренциите на сметката. – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Introduction.htm?tocpath=Administrator%7CComponents%7CSSH%C2%A0Key%20Manager%7C 0
Системот мора да поддржува изолација и следење на сесиите без потреба да се открие лозинката / клучот ssh на привилегираниот корисник на корисничката станица. Кога крајниот корисник е безбедно автентициран на Модулот за раздвојување на системот и е наведен привилегираниот корисник, предложеното решение мора автоматски да ги преземе привилегираните ингеренции од централниот репозиториум, да ја стартува апликацијата избрана претходно од корисникот (апликацијата е инсталирана на модулот за одвојување) и автоматски да ги внесе	Системот поддржува изолација и следење на сесиите без потреба да се открие лозинката / клучот ssh на привилегираниот корисник на корисничката станица. Кога крајниот корисник е безбедно автентициран на Модулот за раздвојување на системот и е наведен привилегираниот корисник, предложеното решение автоматски да ги преземе привилегираните ингеренции од централниот репозиториум, ја стартува апликацијата избрана претходно од корисникот (апликацијата е инсталирана на модулот за одвојување) и автоматски ги внесува ингеренциите во апликацијата (не се дистрибуираат на корисничката работна станица). Снимањето сесии со индексирање на податоци е достапно како опција во дефинирањето на политиките. Во случај на управување со врските на веб-прелистувачот преку системот за одделување модули, го

ингеренциите во апликацијата (да не се дистрибуираат на корисничката работна станица). Снимањето сесии со индексирање на податоци мора да биде достапно како опција во дефинирањето на политиките. Во случај на управување со врските на веб-прелистувачот преку системот за одделување модули, мора да го зацврсти веб-прелистувачот (на пр., да го оневозможи менито за адреси, алатките, да го блокира внесувањето на корисникот за време на процесот на вбризгување акредитиви итн.	зацврстува веб-прелистувачот (на пр., да го оневозможи менито за адреси, алатките, да го блокира внесувањето на корисникот за време на процесот на вбризгување акредитиви итн. – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Privileged-Session%20Manager-Introduction.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7C 0
Системот мора да поддржува изолација и следење на сесиите без потреба да се открие лозинката / клучот ssh на привилегираниот корисник на корисничката станица. Кога крајниот корисник е безбедно автентициран на Модулот за раздвојување на системот и е наведен привилегираниот корисник, предложеното решение мора автоматски да ги преземе привилегираните ингеренции од централниот репозиториум, да ја стартува апликацијата избрана претходно од корисникот (апликацијата е инсталирана на модулот за одвојување) и автоматски да внесе ингеренциите во апликацијата (да не се дистрибуираат на корисничката работна станица). Снимањето сесии со „Системот мора безбедно да воспостави и да управува со привилегирани сесии за не помалку од следниве системи: а) Оперативни системи: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390) б) Бази на податоци: Microsoft SQL, Oracle, MySQL, SAP HANA, HeidiSQL, DB2 в) Системи и апликации за управување со инфраструктурата: DELL DRAC, RSA менаџер за автентикација, HP iLO, SAP GUI, BMC Remedy	Системот поддржува изолација и следење на сесиите без потреба да се открие лозинката / клучот ssh на привилегираниот корисник на корисничката станица. Кога крајниот корисник е безбедно автентициран на Модулот за раздвојување на системот и е наведен привилегираниот корисник, предложеното решение автоматски да ги преземе привилегираните ингеренции од централниот репозиториум, ја стартува апликацијата избрана претходно од корисникот (апликацијата е инсталирана на модулот за одвојување) и автоматски внесува ингеренциите во апликацијата (не се дистрибуираат на корисничката работна станица). Снимањето сесии со „Системот безбедно воспоставува и управува со привилегирани сесии за не помалку од следниве системи: а) Оперативни системи: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390) – https://cyberark-customers.force.com/mplace/s/#---Category c-OperatingSystem~CyberArk Solution c-PrivilegedSessionManagement б) Бази на податоци: Microsoft SQL, Oracle, MySQL, SAP HANA, HeidiSQL, DB2 – https://cyberark-customers.force.com/mplace/s/#---Category c-Database~CyberArk Solution c-PrivilegedSessionManagement в) Системи и апликации за управување со инфраструктурата: DELL DRAC, RSA менаџер за автентикација, HP iLO, SAP GUI, BMC Remedy – https://cyberark-customers.force.com/mplace/s/#---Category c-RemoteAccess~CyberArk Solution c-

г) Мрежни уреди и безбедносни уреди: Cisco (рутери, nexus свичеви, заштитен ѕид), HP, Checkpoint (SmartDashboard, https, ssh), Radware, F5 Networks, FortiGate, Palo Alto Networks д) Алатки за CI/CD (https, ssh): готвач, Џенкинс, Кубернетс, Докер, Jfrog, GitHub ѓ) Веб-услуги: SaaS услуги, веб-интерфејси, минимум: Facebook (на пр. маркетинг сметки), веб-услуги на Amazon (управувачка конзола, IAM, STS интеграција), управување со Microsoft Azure е) Околини за виртуелизација: VMWare ESX/ESXi, vCenter (vSphere Client, https, ssh)	PrivilegedSessionManagement и https://cyberark-customers.force.com/mplace/s/#a3550000000EiCJAA0-a3950000000jjUtAAI и https://cyberark-customers.force.com/mplace/s/#a3550000000ElOgAAK-a3950000000jjvKAAQ и https://cyberark-customers.force.com/mplace/s/#a3550000000Ekj8AAC-a3950000000jjr3AAA г) Мрежни уреди и безбедносни уреди: Cisco (рутери, nexus свичеви, заштитен ѕид), HP, Checkpoint (SmartDashboard, https, ssh), Radware, F5 Networks, FortiGate, Palo Alto Networks - https://cyberark-customers.force.com/mplace/s/#---Category__c-NetworkDevice~CyberArk_Solution__c-PrivilegedSessionManagement и https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Introduction-to-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C_____1 д) Алатки за CI/CD (https, ssh): готвач, Џенкинс, Кубернетс, Докер, Jfrog, GitHub - https://cyberark-customers.force.com/mplace/s/#---Category__c-DevOps~CyberArk_Solution__c-PrivilegedSessionManagement ѓ) Веб-услуги: SaaS услуги, веб-интерфејси, минимум: Facebook (на пр. маркетинг сметки), веб-услуги на Amazon (управувачка конзола, IAM, STS интеграција), управување со Microsoft Azure - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PSMCloudServicesManagementTool.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7CPSM%20Connectors%7CCloud%20Services%20Management%20Tools%7C_____0 е) Околини за виртуелизација: VMWare ESX/ESXi, vCenter (vSphere Client, https, ssh) - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PSM_Virtualization.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7CPSM%20Connectors%7CVirtualization%7C_____0

Модулот за прокси мора да ја поддржува функционалноста на Microsoft Remote App за објавување апликации. Скриптите за стврднување мора да бидат испорачани од продавачот на PAM и да се извршат за време на инсталацијата на производот.	Модулот за прокси ја поддржува функционалноста на Microsoft Remote App за објавување апликации. Скриптите за стврднување ќе бидат испорачани од нас на PAM и ќе се извршат за време на инсталацијата на производот. – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PSM-Architecture.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7C 1
„Системот мора да обезбеди кориснички пристап до заштитениот ресурс со не помалку од следните алатки/методи: а) Веб интерфејс на привилегирано безбедносно решение за акаунтот б) Различни клиенти/менаџери на RDP што се користат на станицата од која се врши привилегиран пристап со не помалку од: дефинирање параметри за поврзување во конфигурацискатa датотека на клиентот RDP или интерактивно барање корисник за својствата на заштитениот систем (како што се адреса, апликација на клиент, привилегирана сметка име). Системот мора да поддржува PKI сертификати како метод за директно автентикација на Separation Module. в) Веб-прелистувач кој поддржува html5 за да обезбеди безбеден кориснички пристап за оперативни системи различни од Windows (без клиент RDP). Привилегираната сесија (мора да биде тунелирана во html5 и достапна за корисникот како нова картичка во прелистувачот. г) Различни командна линија и SSH клиенти (на пр. кит), со автентикација	„Системот ќе обезбеди кориснички пристап до заштитениот ресурс со не помалку од следните алатки/методи: а) Веб интерфејс на привилегирано безбедносно решение за акаунтот – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Password-Vault-Web-Access.htm?tocpath=Administrator%7CComponents%7CPVWA%7C 0 б) Различни клиенти/менаџери на RDP што се користат на станицата од која се врши привилегиран пристап со не помалку од: дефинирање параметри за поврзување во конфигурацискатa датотека на клиентот RDP или интерактивно барање корисник за својствата на заштитениот систем (како што се адреса, апликација на клиент, привилегирана сметка име). Системот мора да поддржува PKI сертификати како метод за директно автентикација на Separation Module. – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PSM-Architecture.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7C 1 и https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/supported-auth-methods.htm?tocpath=Administrator%7CUser%20Management%7CAuthenticate%20to%20Privileged%20Access%20Manager%20-%20Self-

на системот заснована на клучеви SSH."	Hosted%7CConfigure%20authentication%20methods%7C0 в) Веб-прелистувач кој поддржува html5 за да обезбеди безбеден кориснички пристап за оперативни системи различни од Windows (без клиент RDP). Привилегираната сесија (мора да биде тунелирана во html5 и достапна за корисникот како нова картичка во прелистувачот. – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PSM_HTML5.htm г) Различни командна линија и SSH клиенти (на пр. кит), со автентикација на системот заснована на клучеви SSH." – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Privileged-Session-Manager-SSH-Proxy-Introduction.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C0
Системот мора да обезбеди опција за крајниот корисник да избере дали конкретната графичка сесија треба да се воспостави со протокол RDP или HTTPS (сесија тунелирана во HTML5)	Системот ќе обезбеди опција за крајниот корисник да избере дали конкретната графичка сесија треба да се воспостави со протокол RDP или HTTPS (сесија тунелирана во HTML5) - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PSM-Architecture.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7C1
Системот мора да обезбеди временски ограничен привилегиран пристап со привремено доделување акаунт на Windows (локален или домен) на група локални администратори по поднесување соодветно барање (Пристап само на време). Дозволите доделени од Системот мора автоматски да се деактивираат по надминување на одобрената временска рамка за подигање на привилегиите.	Системот ќе обезбеди временски ограничен привилегиран пристап со привремено доделување акаунт на Windows (локален или домен) на група локални администратори по поднесување соодветно барање (Пристап само на време). Дозволите доделени од Системот автоматски ќе се деактивираат по надминување на одобрената временска рамка за подигање на привилегиите. - https://www.cyberark.com/what-is/just-in-time-access/

По повеќефакторската автентикација на системот за графички интерфејс мора да обезбеди функционалност за генерирање и преземање приватен SSH клуч (системот мора да обезбеди полиса за декларација за време на важност на клучот) за да се овозможи безбеден пристап до целните средства преку прокси-модулот без потреба да се обезбедат дополнителни фактори за автентикација. Мора да се обезбеди пристап до целните системи врз основа на RBAC доделен на корисникот кој го генерирал и преземал SSH. Системот мора да обезбеди заштита на лозинка за генерирани SSH клучеви со дефинирана должина и сложеност на лозинката.	По повеќефакторската автентикација на системот за графички интерфејс ќе се обезбеди функционалност за генерирање и преземање приватен SSH клуч (системот мора да обезбеди полиса за декларација за време на важност на клучот) за да се овозможи безбеден пристап до целните средства преку прокси-модулот без потреба да се обезбедат дополнителни фактори за автентикација. Ќе се обезбеди пристап до целните системи врз основа на RBAC доделен на корисникот кој го генерирал и преземал SSH. Системот ќе обезбеди заштита на лозинка за генерирани SSH клучеви со дефинирана должина и сложеност на лозинката. - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/RADIUS-Authentication.htm?tocpath=Administrator%7CUser%20Management%7CAuthenticate%20to%20Privileged%20Access%20Manager%20-%20Self-Hosted%7CConfigure%20authentication%20methods%7C 4 и https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Introduction.htm?tocpath=Administrator%7CComponents%7CSSH%C2%A0Key%20Manager%7C 0
Управување со безбедносни инциденти	
Системот мора да обезбеди категоризација на снимените кориснички сесии со претходно дефинирани нивоа на ризик. Ризикот мора да се дефинира врз основа на збир на политики на функции/команди откриени за време на сесијата и тежината што им е доделена. Ризикот мора автоматски да се анализира за време на тековните сесии. Информациите за нивото на ризик доделено на сесијата мора да бидат видливи и во конзолата за следење на сесиите и во интерфејсот на контролната табла за безбедносни инциденти. Администраторот мора да може да одреди кои дејства што ги врши корисникот треба автоматски да бидат суспендирани или прекинати.	Системот ќе обезбеди категоризација на снимените кориснички сесии со претходно дефинирани нивоа на ризик. Ризикот се дефинира врз основа на збир на политики на функции/команди откриени за време на сесијата и тежината што им е доделена. Ризикот автоматски да се анализира за време на тековните сесии. Информациите за нивото на ризик доделено на сесијата се видливи и во конзолата за следење на сесиите и во интерфејсот на контролната табла за безбедносни инциденти. Администраторот ќе одреди кои дејства што ги врши корисникот треба автоматски да бидат суспендирани или прекинати. - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Analyzing-High-Risk-Activities-during-PSM-Sessions.htm и https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/PTA/Viewing-Privileged-Related-Risks.htm

Системот мора да има вградени аналитички алатки кои овозможуваат автоматско (без барање за рачно дефинирање правила за безбедносна политика) откривање на сомнителни активности на привилегирани корисници. Откривањето мора да се потпира на автоматски научено однесување на поединечни корисници (стандардно работно време, опсег на IP адреса, количина на референци до складиштето на профилот за преземање лозинки).	Системот има вградени аналитички алатки кои овозможуваат автоматско (без барање за рачно дефинирање правила за безбедносна политика) откривање на сомнителни активности на привилегирани корисници. Откривањето се потпира на автоматски научено однесување на поединечни корисници (стандардно работно време, опсег на IP адреса, количина на референци до складиштето на профилот за преземање лозинки). – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/Landing%20Pages/lp_ThreatAnalyticsUser.htm
Системот треба да собира и анализира податоци за активноста на корисникот од надворешни SIEM системи, не помалку од следниве решенија мора да бидат поддржани: Arcsight, Qradar, Splunk, LogRhythm, RSA, McAfee и оперативни системи: rsyslog (од Unix / Linux системи), Windows Event Препраќач (од Windows системи), AWS CloudTrail, апликација Azure Function.	Системот собира и анализира податоци за активноста на корисникот од надворешни SIEM системи, поддржани се: Arcsight, Qradar, Splunk, LogRhythm, RSA, McAfee и оперативни системи: rsyslog (од Unix / Linux системи), Windows Event Препраќач (од Windows системи), AWS CloudTrail, апликација Azure Function. – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Inbound-Forwarding-Data-to-PTA.htm и https://cyberark-customers.force.com/mplace/s/#---CyberArk_Solution__c-AnalyticsAndThreatDetection
Системот мора да има опција за поправка и извршување на дејството за одговор (барем принудувајќи ја да се смени лозинката за привилегираниот кориснички профил) ако се открие сомнително користење на привилегираниот акаунт (кражба на акредитиви на привилегираниот акаунт или создавање нов привилегиран акаунт).	Системот има опција за поправка и извршување на дејството за одговор (барем принудувајќи ја да се смени лозинката за привилегираниот кориснички профил) ако се открие сомнително користење на привилегираниот акаунт (кражба на акредитиви на привилегираниот акаунт или создавање нов привилегиран акаунт). - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/PTA/Security-Configuration.htm
Системот мора да генерира соодветен аларм во случај на откривање прекумерно користење на привилегирани акаунти и во случај на користење на привилегираниот акаунт во нестандардни часови (на пр.	Системот генерира соодветен аларм во случај на откривање прекумерно користење на привилегирани акаунти и во случај на користење на привилегираниот акаунт во нестандардни часови (на пр. надвор од работното време типично за даден корисник) - https://docs.cyberark.com/Product-

надвор од работното време типично за даден корисник)	Doc/OnlineHelp/PAS/11.3/en/Content/PTA/What-Does-PTA-Detect.htm
Системот треба да открие инцидент кога привилегираните ингеренции се користат за директно поврзување со целниот систем (без добивање лозинка од заштитеното складиште) и настан кога се креира нов привилегиран акаунт во системот. За безбедносните настани опишани во оваа точка системот мора да обезбеди процедури за автоматска санација, не помалку од: ресетирање на лозинка за привилегираниот акаунт кога ќе се случи безбедносен инцидент, автоматско (неуправувано) вклучување на акаунтот и автоматско усогласување на лозинките.	Системот открива инцидент кога привилегираните ингеренции се користат за директно поврзување со целниот систем (без добивање лозинка од заштитеното складиште) и настан кога се креира нов привилегиран акаунт во системот. За безбедносните настани опишани во оваа точка системот обезбедува процедури за автоматска санација, не помалку од: ресетирање на лозинка за привилегираниот акаунт кога ќе се случи безбедносен инцидент, автоматско (неуправувано) вклучување на акаунтот и автоматско усогласување на лозинките. - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/PTA/What-Does-PTA-Detect.htm и https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/PTA/Security-Configuration.htm
Системот мора да може да детектира нови неуправувани привилегирани профили и врски низ AWS и Azure околината што биле воспоставени без да ја преземе лозинката од централното складиште.	Системот може да детектира нови неуправувани привилегирани профили и врски низ AWS и Azure околината што биле воспоставени без да ја преземе лозинката од централното складиште. - https://cyberark-customers.force.com/mplace/s/#a352J000000d907QAA-a392J000001Z3WFQA0
Системот мора да обезбеди функционалности на ревизорот за: следење на тековната сесија, суспендирање / прекинување на сесиите, дефинирање група настани (наредби, стартување апликација итн.) за кои системот автоматски треба да ја заврши / суспендира сесијата (функцијата за завршување / суспендирање на сесијата мора да биде достапна барем за внатрешни претплата / лиценца за вработени)	Системот може да обезбеди функционалности на ревизорот за: следење на тековната сесија, суспендирање / прекинување на сесиите, дефинирање група настани (наредби, стартување апликација итн.) за кои системот автоматски треба да ја заврши / суспендира сесијата (функцијата за завршување / суспендирање на сесијата се достапни барем за внатрешни претплата / лиценца за вработени) - https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/NewUI/NewUI-Monitor-sessions.htm
Архитектура	

Системот мора да обезбеди опција за инсталирање на базата на податоци на централно складиште за акредитиви на одвоен, зацврстен оперативен систем што нема да биде споделен со други модули, како што се нас: прокси за изолација на сесија, веб-интерфејс, аналитички модул, мотор за ротација на лозинка.	Системот обезбедува опција за инсталирање на базата на податоци на централно складиште за акредитиви на одвоен, зацврстен оперативен систем што нема да биде споделен со други модули, како што се нас: прокси за изолација на сесија, веб-интерфејс, аналитички модул, мотор за ротација на лозинка. – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/Security/Security%20Fundamentals-Introduction.htm
Целото решение мора да биде обезбедено од истиот производител, поединечните функционални модули мора да се интегрираат едни со други	Целото решение е обезбедено од истиот производител, поединечните функционални модули се интегрираат едни со други – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/Landing%20Pages/LPAdministerComponents.htm
Системот мора да биде модуларен, со компоненти за проширување достапни под посебни претплати / лиценци, за не помалку од: - мултифакторска автентикација и управување со пристап до веб-апликации и безбедност (за внатрешни и апликации базирани на облак) со доставување на функционалност за еднократно пријавување - заштита од далечински пристап за вработените и надворешните добавувачи, барања - интеграција со надворешни комерцијални системи како IAM, RPA, алатки за ранливост, - Спроведување на најмала привилегија врз основа на агенти на станиците на Windows со бришење локални администраторски сметки и зголемување на правата во контекст на специфични објекти (скрипти,	Системот е модуларен, со компоненти за проширување достапни под посебни претплати / лиценци, а не помалку од: - мултифакторска автентикација и управување со пристап до веб-апликации и безбедност (за внатрешни и апликации базирани на облак) со доставување на функционалност за еднократно пријавување - заштита од далечински пристап за вработените и надворешните добавувачи, барања - интеграција со надворешни комерцијални системи како IAM, RPA, алатки за ранливост, - Спроведување на најмала привилегија врз основа на агенти на станиците на Windows со бришење локални администраторски сметки и зголемување на правата во контекст на специфични објекти (скрипти, апликации, инсталации, dll и друго) за одредени корисници, контрола на апликации и блокирање на протекување на ингеренциите (на пр. лозинки) од складишта и апликации на оперативниот систем Windows (на пр. веб-прелистувачи, LSASS меморија, SAM и други), - заштита на тајните во средини DevOps

апликации, инсталации, dll и друго) за одредени корисници, контрола на апликации и блокирање на протекување на ингеренциите (на пр. лозинки) од складишта и апликации на оперативниот систем Windows (на пр. веб-прелистувачи, LSASS меморија, SAM и други), - заштита на тајните во средини DevOps - заштита на привилегирани сметки вградени во статични апликации и административни скрипти - управување со правата во Cloud платформи - Спроведување на најмала привилегија базирано на агенти на серверите Linux / Unix (централно управување со дозволеното / недозволено извршување команда, централно покачување на привилегијата, корисничка одговорност, снимање на локална сесија), барања - модул кој овозможува складирање на ингеренциите на деловните корисници во складиштето за лозинки	- заштита на привилегирани сметки вградени во статични апликации и административни скрипти - управување со правата во Cloud платформи - Спроведување на најмала привилегија базирано на агенти на серверите Linux / Unix (централно управување со дозволеното / недозволено извршување команда, централно покачување на привилегијата, корисничка одговорност, снимање на локална сесија), барања - модул кој овозможува складирање на ингеренциите на деловните корисници во складиштето за лозинки – https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/Landing%20Pages/LPAdministerComponents.htm
Добавувачот на PAM мора да обезбеди процедури кои го опишуваат методот на подобрување на секоја од компонентите на системот и да обезбеди скрипти кои го автоматизираат процесот на зацврстување на безбедноста во инсталационите пакети, приспособени на секој од функционалните модули. Подобрувањето на секоја од компонентите мора да се изврши во согласност со најдобрите практики на производителот на оперативниот систем и производителот на растворот PAM/PAS. Подобрувањето на оперативниот систем на складиштето за акредитиви мора да се изврши автоматски од страна на	Ќе обезбедиме процедури кои го опишуваат методот на подобрување на секоја од компонентите на системот и да обезбеди скрипти кои го автоматизираат процесот на зацврстување на безбедноста во инсталационите пакети, приспособени на секој од функционалните модули. Подобрувањето на секоја од компонентите ќе се изврши во согласност со најдобрите практики на производителот на оперативниот систем и производителот на растворот PAM/PAS. Подобрувањето на оперативниот систем на складиштето за акредитиви мора ќе изврши автоматски од страна на инсталерот за време на процесот на инсталација на модулот.

инсталерот за време на процесот на инсталација на модулот.	https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/Resources/_TopNav/cc_Home.htm
Системот треба да вклучува не помалку од: еден модул за складиште за лозинки, 5x модул за складиште за целите на враќање од катастрофи / висока достапност, 5x модул за промени и управување со клучеви и лозинки во заштитените системи, 2 тест околини што овозможуваат мапирање на производната средина.	Системот вклучува не помалку од: еден модул за складиште за лозинки, 5x модул за складиште за целите на враќање од катастрофи / висока достапност, 5x модул за промени и управување со клучеви и лозинки во заштитените системи, 2 тест околини што овозможуваат мапирање на производната средина. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PSM-Disaster-Recovery.htm
Решението не може да го ограничи бројот на модули што се користат за изолација на сесиите на следење, како и веб-кориснички интерфејси на решението (додавањето дополнителни модули нема да бара купување дополнителни лиценци / претплати од Добавувачот на системот PAM).	Решението не го ограничува бројот на модули што се користат за изолација на сесиите на следење, како и веб-кориснички интерфејси на решението (додавањето дополнителни модули нема да бара купување дополнителни лиценци / претплати од Добавувачот на системот PAM).
Системот мора да поддржува дистрибуирана архитектура, во која поединечни функционални модули (прокси-прокси, модули за тајно ротирање, интерфејси WebUI) се инсталирани на повеќе локации (географски одвоени) и комуницираат со централните елементи (складиште за акредитиви) користејќи безбеден протокол за комуникација (обезбедување податоци безбедност за време на преносот, работи преку една TCP порта, која може да се декларира при инсталирање на системот). Во случај на дистрибуирана инфраструктура, целиот систем мора да се управува од централен графички интерфејс	Системот поддржува дистрибуирана архитектура, во која поединечни функционални модули (прокси-прокси, модули за тајно ротирање, интерфејси WebUI) се инсталирани на повеќе локации (географски одвоени) и комуницираат со централните елементи (складиште за акредитиви) користејќи безбеден протокол за комуникација (обезбедување податоци безбедност за време на преносот, работи преку една TCP порта, која може да се декларира при инсталирање на системот). Во случај на дистрибуирана инфраструктура, целиот систем мора да се управува од централен графички интерфејс https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Managing-the-CyberArk-License.htm?TocPath=Administrator%7CComponents%7CDigital%20Vault%7COperate%20the%20CyberArk%20Vault%7C_8
Високата достапност на модулот за складирање привилегирани сметки мора да се имплементира на слојот на	Високата достапност на модулот за складирање привилегирани сметки ќе се имплементира на слојот на

предложениот софтвер (апликација), а не на оперативниот систем / базата на податоци на кој е инсталиран софтверот	предложениот софтвер (апликација), а не на оперативниот систем / базата на податоци на кој е инсталиран софтверот https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PSM-Disaster-Recovery.htm
Производот мора да обезбеди криптографска заштита за резервните копии генерирани од производот	Производот ќе обезбеди криптографска заштита за резервните копии генерирани од производот https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/Security/Security%20Fundamentals-Introduction.htm?tocpath=Security%7C_____1
Решението мора да обезбеди функционалност за имплементирање на модулите за складирање на привилегирани сметки во дистрибуирана форма, заснована на: активен модул, вишок на активниот модул и збир на активни географски распределени модули, обезбедувајќи (во режим на читање) најкритични функции за крајните корисници. (на пр. механизми за резервна копија, споделување податоци за привилегирани сметки со апликации, пристап до корисничкиот интерфејс, воспоставување привилегирани сесии на безбеден начин). Предложеното решение мора да поддржува не помалку од 6 активни складишта за акредитиви. Во случај на дистрибуирана инфраструктура, целиот систем мора да се управува од централен графички интерфејс.	Решението обезбедува функционалност за имплементирање на модулите за складирање на привилегирани сметки во дистрибуирана форма, заснована на: активен модул, вишок на активниот модул и збир на активни географски распределени модули, обезбедувајќи (во режим на читање) најкритични функции за крајните корисници. (на пр. механизми за резервна копија, споделување податоци за привилегирани сметки со апликации, пристап до корисничкиот интерфејс, воспоставување привилегирани сесии на безбеден начин). Предложеното решение поддржува не помалку од 6 активни складишта за акредитиви. Во случај на дистрибуирана инфраструктура, целиот систем се управува од централен графички интерфејс. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Distributed-Vaults-Introduction.htm
Репозиториумот во кој се чуваат заштитени привилегирани акаунти мора да се доставува со резервни компоненти за враќање од катастрофи на географски одвоени локации. Мора да биде можно да се користат не помалку од следниве методи за висока достапност и враќање при катастрофи: а) режимот на висока достапност помеѓу два тајни системи на складиште кои го делат просторот на дискот со шифрирана база на податоци	Репозиториумот во кој се чуваат заштитени привилегирани акаунти се доставува со резервни компоненти за враќање од катастрофи на географски одвоени локации. Можно е да се користат не помалку од следниве методи за висока достапност и враќање при катастрофи: а) режимот на висока достапност помеѓу два тајни системи на складиште кои го делат просторот на дискот со шифрирана база на податоци б) модули за враќање од катастрофи на други локации (мора да биде можно да се имплементираат до 4 модули за враќање од катастрофи како дел од

б) модули за враќање од катастрофи на други локации (мора да биде можно да се имплементираат до 4 модули за враќање од катастрофи како дел од основната претплата со распореденият НА на примарната локација) Мора да биде возможно да се имплементираат двата опишани методи (а и б) во иста производна средина“.	основната претплата со распореденият НА на примарната локација) Возможно е да се имплементираат двата опишани методи (а и б) во иста производна средина“. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PSM-Disaster-Recovery.htm
Решението мора да обезбеди “breaking glass offline” пристап до привилегирани тајни во посветена мобилна апликација (достапна на оперативните системи IOS и Android). Системскиот администратор мора да може да дефинира ситуации во кои ќе се активира офлајн пристапот, не помалку отколку за следните сценарија: не е достапна мрежна врска од мобилната апликација, кога услугата за пристап не е достапна, администраторот мора да може да одреди дали офлајн пристапот е достапни само за корисници на компанијата или, исто така, продавачи од трета страна.	Решението обезбедува “breaking glass offline” пристап до привилегирани тајни во посветена мобилна апликација (достапна на оперативните системи IOS и Android). Системскиот администратор може да дефинира ситуации во кои ќе се активира офлајн пристапот, не помалку отколку за следните сценарија: не е достапна мрежна врска од мобилната апликација, кога услугата за пристап не е достапна, администраторот може да одреди дали офлајн пристапот е достапни само за корисници на компанијата или, исто така, продавачи од трета страна. https://cyberark-customers.force.com/s/question/0D52J00006ZYQVrSAP/break-glass-procedure
Интеграција	
Системот мора да обезбеди можност за интегрирање со SIEM решенијата за испраќање информации за регистрирани настани како дел од набљудуваните сесии. Системот мора да обезбеди можност да конфигурира какви видови настани треба да се испраќаат до системот SIEM.	Системот обезбедува можност за интегрирање со SIEM решенијата за испраќање информации за регистрирани настани како дел од набљудуваните сесии. Системот обезбедува можност да конфигурира какви видови настани треба да се испраќаат до системот SIEM. https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-connect-siem.htm
Системот мора да обезбеди интеграција со системите за отврање на инциденти, не помалку од: BMC Remedy, ServiceNow и друго преку отворено API, сфатено како потврда дали постои точен инцидент во	Системот обезбедува интеграција со системите за отврање на инциденти, не помалку од: BMC Remedy, ServiceNow и друго преку отворено API, сфатено како потврда дали постои точен инцидент во системот за инциденти и дали има соодветен статус за да може да се дозволи пристап за

системот за инциденти и дали има соодветен статус за да може да се дозволи пристап за примање привилегирани ингеренциите или воспоставете привилегирана врска	примање привилегирани ингеренциите или воспоставете привилегирана врска – https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-serviceNow.htm
Системот мора да обезбеди интеграција со HSM-уреди базирани на PKCS#11, не помалку од: Atos HSM Proteccio, Gemalto Luna/Safenet 1700 Хардверски безбедносен модул, Thales nShield Хардверски безбедносен модул, Utimaco CryptoServer, Crypto4A QxEDGE, Fortanix Unident TSDK Контрола, Utimaco CryptoServer.	Системот обезбедува интеграција со HSM-уреди базирани на PKCS#11, не помалку од: Atos HSM Proteccio, Gemalto Luna/Safenet 1700 Хардверски безбедносен модул, Thales nShield Хардверски безбедносен модул, Utimaco CryptoServer, Crypto4A QxEDGE, Fortanix Unident TSDK Контрола, Utimaco CryptoServer. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Intro-Distributed-Vault-HSM.htm
Системот обезбедува интеграција со голем број методи за автентикација, не само лозинки, LDAP, Windows NTLM, SSH клучеви, паметни картички, PKI, RADIUS, SAML, MFA, RSA SecurID, Oracle SSO, Amazon Cognito Authentication, OpenID Connect (OIDC)	Системот обезбедува интеграција со голем број методи за автентикација, не само лозинки, LDAP, Windows NTLM, SSH клучеви, паметни картички, PKI, RADIUS, SAML, MFA, RSA SecurID, Oracle SSO, Amazon Cognito Authentication, OpenID Connect (OIDC) https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/supported-auth-methods.htm?tocpath=Administrator%7CUser%20Management%7CAuthenticate%20to%20Privileged%20Access%20Manager%20-%20Self-Hosted%7CConfigure%20authentication%20methods%7C_____0
Дополнителни карактеристики и функционалности	
Официјалната методологија за имплементација треба да биде достапна на веб-страницата на производителот. Оваа методологија мора да го опфати описот на главните чекори што треба да се преземат за правилно и сеопфатно имплементирање на PAS решение со: заштита на привилегиран пристап, спроведување политика на најмалку привилегии за работни станици и сервери и заштита на привилегирани акаунти и	Официјалната методологија за имплементација е достапна на веб-страницата на производителот. Оваа методологија го опфаќа описот на главните чекори што треба да се преземат за правилно и сеопфатно имплементирање на PAS решение со: заштита на привилегиран пристап, спроведување политика на најмалку привилегии за работни станици и сервери и заштита на привилегирани акаунти и тајни што ги користат апликациите за пристап до други целни системи (вклучувајќи заштита на средини управувани од DevOps). Клучните привилегирани типови сметки се класифицираат и се засноваат на анализа на ризик.

тајни што ги користат апликациите за пристап до други целни системи (вклучувајќи заштита на средини управувани од DevOps). Клучните привилегирани типови сметки треба да се класифицираат и да се засноваат на анализа на ризик. Методологијата мора да биде достапна на официјалната веб-страница на производителот, а кон понудата треба да се приложи линк до официјалната веб-страница на производителот што содржи опис на методологијата.	Методологијата е достапна на официјалната веб-страница на производителот, а кон понудата приложуваме линк до официјалната веб-страница на производителот што содржи опис на методологијата. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/Resources/_TopNav/cc_Home.htm
Предложеното решение треба да се наоѓа во квадрантот „Лидери“ од извештајот Gartner Magic Quadrant for Privileged Access Management.	Предложеното решение се наоѓа во квадрантот „Лидери“ од извештајот Gartner Magic Quadrant for Privileged Access Management. https://www.cyberark.com/press/cyberark-named-a-leader-in-2022-gartner-magic-quadrant-for-privileged-access-management/
Системот треба да обезбеди централно управување со политиките (централна дефиниција на бели листи/црни листи на команди со параметри, доделени на привилегирани сметки и групи луѓе) за мрежен и локален привилегиран пристап за Linux/Unix сервери.	Системот обезбедува централно управување со политиките (централна дефиниција на бели листи/црни листи на команди со параметри, доделени на привилегирани сметки и групи луѓе) за мрежен и локален привилегиран пристап за Linux/Unix сервери. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security-Configuration.htm
Системот треба да обезбеди SUDO централизирана функционалност за замена	Системот обезбедува SUDO централизирана функционалност за замена https://www.cyberark.com/resources/best-practices-for-privileged-access-management/solution-brief-to-sudo-or-not-to-sudo-that-is-the-question
Системот треба да обезбеди снимање на локални сесии и кориснички команди. Кога сесијата ќе заврши, снимките треба да се складираат на безбеден шифриран начин во централното складиште.	Системот обезбедува снимање на локални сесии и кориснички команди. Кога сесијата ќе заврши, снимките се складираат на безбеден шифриран начин во централното складиште. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Configuring-Recordings-and-Audits-in-PSM.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7CConfiguration%7C_____5

Системот треба да обезбеди функционалност за спроведување на управувањето со командите со нивните дополнителни параметри и доделување политика на групите	Системот обезбедува функционалност за спроведување на управувањето со командите со нивните дополнителни параметри и доделување политика на групите https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Installing-the-Remote-Control-Client.htm
Системот треба да ги заштити логовите од отстранување/модификации.	Системот ги заштитува логовите од отстранување/модификации. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/Security/Standards-CyberArks%20Digital%20Vault%20Server%20Security%20Standard.htm?tocpath=Security%7CDigital%20Vault%20Security%20Standard%7C____0
Системот треба да спречи т.н. shell escape (корисниците не можат да извршат ограничена команда од друга програма, на пример: извршете ограничена команда од уредувачот vi отворен со зголемени права).	Системот спречува т.н. shell escape (корисниците не можат да извршат ограничена команда од друга програма, на пример: извршете ограничена команда од уредувачот vi отворен со зголемени права). https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Privileged-Commands-Restrictions.htm
Системот треба да обезбеди опција за интегриран Unix/Linux сервер со AD околина со вградена функционалност AD Bridge (OPM PAM).	Системот обезбедува опција за интегриран Unix/Linux сервер со AD околина со вградена функционалност AD Bridge (OPM PAM). https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/AD-Bridge-for-NIX.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7CAD%20Bridge%20for%20*NIX%20in%20PSM%20for%20SSH%7C____0
Системот мора да обезбеди интеграција помеѓу безбедносниот модул за идентитет и складиштето за лозинки за безбедно складирање на тајните на деловните корисници и автоматски да ги вбризга преку приклучок во прелистувачот на корисникот на веб-апликации достапни на порталот SSO (Single sign on)	Системот обезбедува интеграција помеѓу безбедносниот модул за идентитет и складиштето за лозинки за безбедно складирање на тајните на деловните корисници и автоматски да ги вбризга преку приклучок во прелистувачот на корисникот на веб-апликации достапни на порталот SSO (Single sign on) https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/Applications/BrowserExtension/BrowserExtension-install.htm
Системот мора автоматски да ги препознава посетите на нови деловни веб-локации каде од корисникот ќе биде побарано автентикација. Ингеренциите обезбедени од корисникот мора да се	Системот автоматски да ги препознава посетите на нови деловни веб-локации каде од корисникот ќе биде побарано автентикација. Ингеренциите обезбедени од корисникот можат да се фатат и да се зачуваат во складиштето за лозинки и соодветната нова веб-

фатат и да се зачуваат во складиштето за лозинки и соодветната нова веб-апликација мора да се додаде во каталогот на апликации на порталот SSO (Single sign on).	апликација мора да се додаде во каталогот на апликации на порталот SSO (Single sign on). https://docs.cyberark.com/Product-Doc/OnlineHelp/EPM/22.5/en/Content/IdentityIntegration/Implement-Identity-SSO.htm
Системот мора да го обезбеди приклучокот на корисничкиот прелистувач со вградена функција за генерирање лозинки. Генераторот на лозинки мора да дозволи да се специфицира најмалку должината на лозинката и сложеноста на новогенерираната лозинка (системот мора да дозволи да избере дали броевите, симболите, големите и малите букви треба да се користат во новогенерирана лозинка).	Системот го обезбедува приклучокот на корисничкиот прелистувач со вградена функција за генерирање лозинки. Генераторот на лозинки дозволува да се специфицира најмалку должината на лозинката и сложеноста на новогенерираната лозинка (системот мора да дозволи да избере дали броевите, симболите, големите и малите букви се користат во новогенерирана лозинка). https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/UserPortal/Browser-Extension.htm
Системот мора да обезбеди дополнителна компонента (со дополнителна претплата, која не е вклучена во тековната фаза на проектот) како продолжување на модулот за SSO (Single sign on)што овозможува барем: а) запишете ги сите кориснички активности користејќи "stepper" пристап, . Системот мора да активира слика од екранот на прозорецот на прелистувачот на корисникот заедно со релевантните метаподатоци за барем следните дејства што ги прави корисникот за време на набљудуваната веб-сесија: кликнувања на глувчето, притискање на тастатурата „enter" или „tab". Системот мора да дозволи да се пребаруваат сите снимени сесии користејќи бесплатно внесување текст и да ги филтрира безбедносните настани по датуми и дејства. б) идентификувајте кога сесијата со висок ризик е оставена отворена и	Системот обезбедува дополнителна компонента (со дополнителна претплата, која не е вклучена во тековната фаза на проектот) како продолжување на модулот за SSO (Single sign on)што овозможува барем: а) запишете ги сите кориснички активности користејќи "stepper" пристап, . Системот мора да активира слика од екранот на прозорецот на прелистувачот на корисникот заедно со релевантните метаподатоци за барем следните дејства што ги прави корисникот за време на набљудуваната веб-сесија: кликнувања на глувчето, притискање на тастатурата „enter" или „tab". Системот дозволува да се пребаруваат сите снимени сесии користејќи бесплатно внесување текст и да ги филтрира безбедносните настани по датуми и дејства. б) идентификувајте кога сесијата со висок ризик е оставена отворена и бара повторна автентикација за да се осигура дека лицето кое ја иницирало веб-сесијата е овластено, в) заштита на веб-сесијата на крајната точка со екстензијата на прелистувачот https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/GetStarted/Welcome.htm?tocpath=Get%20Started%7C_____0

бара повторна автентикација за да се осигура дека лицето кое ја иницирало веб-сесијата е овластено, в) заштита на веб-сесијата на крајната точка со екстензијата на прелистувачот	

Дел III - ФИНАНСИСКА ПОНУДА

III.1. Вкупната цена на нашата понуда, вклучувајќи ги сите трошоци и попусти, без ДДВ, изнесува: 1,890,000.00 денари *[со бројки]* еденмилионосумстотинидеведесестилјади *[со букви]* денари. Вкупниот износ на ДДВ изнесува 340,200.00 денари [*со бројки*] тристачетириесетилјадиидвеста [*со букви*] денари.

III.2. Нашата понуда важи за периодот утврден во тендерската документација.
III.3. Се согласуваме со начинот и рокот на плаќање утврден во тендерската документација.
III.4. Ги прифаќаме начинот, местото и рокот за испорака на предметната стока, наведени во тендерската документација.
III.5. Со поднесување на оваа понуда, во целост ги прифаќаме условите предвидени во тендерската документација и не го оспоруваме Вашето право да ја поништите постапката за доделување на договор за јавна набавка согласно со член 114 од Законот за јавните набавки.

Дел IV - СОСТАВНИ ДЕЛОВИ НА ПОНУДАТА:

IV.1. Нашата понуда е составена од следниве делови:

1. ОПШТ ДЕЛ,
2. ТЕХНИЧКА ПОНУДА,
3. ФИНАНСИСКА ПОНУДА,
4. ПРИЛОЗИ:

- Пополнет образец на понуда (Прилог 1),
- Изјава за сериозност (Прилог 3),
- Изјава за докажување способност (Прилог 4) или Документи од точка 5.2 и Документи за докажување на способност од точка 5.3,

Место и датум

Скопје, 01.11.2022

Одговорно лице

_____

(потпис*)

**Овој образец не се потпишува своерачно, туку исклучиво електронски со прикачување на валиден дигитален сертификат чиј носител е одговорното лице или лице овластено од него.*