Блок: **Информационни технологии**

Система:

Подразделение: **П**

УТВЪРЖДАВАМ,

ЗАМЕСТНИК-ИЗПЪЛНИТЕЛЕН ДИРЕКТОР,

Заличено на основание ЗЗЛД

СЪГЛАСУВАЛИ:

ДИРЕКТОР "БЕЗОПАСНОСТ И

09.01.2024 г. /ДАРИУШ Н

ДИРЕКТОР "ПРОИЗВОДСТВО"

08.01.2024 г. /АТАНАС АТАНАСОВ/

ТЕХНИЧЕСКО ЗАДАНИЕ

№ 23.П.ТЗ.374

За проектиране и изграждане на строеж и/или проектиране, доставка, монтаж и въвеждане в експлоатация

ТЕМА: Внедряване на система за защита от кибератаки, обхващащи комуникационните и информационни системи на „АЕЦ Козлодуй“ ЕАД

Настоящото техническо задание съдържа техническа спецификация съгласно Закона за обществените поръчки.

1. Кратко описание на техническото задание

Съгласно Закон за киберсигурност (чл. 4, ал. 1, т. 2) „АЕЦ Козлодуй“ е оператор на обществени услуги и като такъв трябва да прилага (чл. 21, ал. 2, т. 2) подходящи мерки за предотвратяване и намаляване до минимум на въздействието на инцидентите, засягащи мрежовата и информационната сигурност, с цел осигуряване на непрекъснатост на дейността им.

Предмет на техническото задание е разработване и реализиране на проект за внедряване на цялостна система чрез която да се реализира мониторинг в реално време, откриване на киберзаплахи, реакция и разследване на инциденти, които могат да нанесат както обратими, така и необратими последствия върху комуникационните и информационните системи на дружеството. Осигуряване на хардуерна и софтуерна поддръжка на внедрените системи.

С внедряване на системата за киберзащита в инфраструктурата на АЕЦ „Козлодуй“ ще бъде постигнато цялостно повишаване нивото на информационна сигурност, включително:

- откриване на известни и неизвестни заплахи с помощта на поведенчески анализи за подобряване на точността и намаляване на времето за реакция (разследване и реакция в

рамките на минути вместо дни);
- автоматизиране на разследването и реакцията с помощта на предварително изградени сценарии за инциденти;
- централизиране на работните процеси за откриване, разследване и реагиране в един потребителски интерфейс;
- постигане на съответствие с чл. 28, чл. 29, чл. 30 и чл. 31 от „Наредба за минималните изисквания за мрежова и информационна сигурност".

Общият срок за изпълнение на всички дейности е до 225 (двеста двадесет и пет) календарни дни, както следва:

- За проектиране – до 85 календарни дни (от датата на сключване на договора), в това число:

• Входни данни - 40 календарни дни (10 календарни дни за поискване на входни данни + 30 календарни дни за предоставяне).

• За Работен проект - до 45 (четиридесет и пет) календарни дни (от датата на протокол за предаване и приемане на входни данни);

- За етап "Доставка" - 80 (осемдесет) календарни дни след приемане на работния проект без забележки;

- Срок за изпълнение на услугите по **инсталиране, активиране и въвеждане в експлоатация** не по-късно от 50 (петдесет) календарни дни, след приемане дейностите по доставка без забележки.

- Срок за обучение за администриране и конфигуриране на системите не по-късно от 10 (десет) календарни дни, считано от приключване изпълнението на дейностите по инсталиране, активиране и въвеждане в експлоатация.

2. Изисквания към проекта

Системата за защита от кибератаки трябва да включва следните модули:

- Система за анализ на събития чрез събиране, наблюдение и анализ на логовете в информационната система или „Security Information and Event Management (SIEM)";
- Система за реакция, управление и автоматизация на решенията за сигурност или Security Orchestration, Automation & Response (SOAR);
- Платформа за разузнаване на заплахи;
- Платформа за киберзащита на крайни точки;
- Платформа за управление на акаунти и привилегирован достъп;
- Система, осигуряваща възможност за отдалечен достъп през криптиран канал за комуникация с включени функционалности за инспекция, защита на крайни устройства и VPN без агент (Clientless VPN);

Основни функции, които трябва да изпълнява системата за защита от кибератаки са:

- да се елиминира или ограничи до минимум възможността за неоторизиран достъп и/или компрометиране на информационните системи;
- да не допуска неоторизирани действия;
- да осигурява защита на информационните системи от външни и вътрешни намеси, които могат да нарушат работата им;
- да извършва анализ на информационната система срещу конвенционални и съвременни сложни киберзаплахи;
- да осигурява управление на събития и инциденти, свързани със киберсигурността на информационната система;

- да осигурява управление и защита на привилегировани потребители и акаунти;
- да предоставя интерактивно разследване на инциденти, сътрудничество между отделните екипи и анализатори, документиране и исторически преглед на извършените действия;
- да осигурява управление и наблюдение на всички защитени крайни точки;
- да осигурява отдалечен достъп до информационната система през криптиран канал за комуникация.

Обхват на система за защита от кибератаки

Информационната система на АЕЦ „Козлодуй“, изградена на база на Microsoft AD. Системата за защита от кибератаки не обхваща технологичните информационни системи пряко свързани с експлоатацията на ядрените мощности.

2.1. Описание на изискванията към отделните части на проекта

Проектът да се разработи еднофазно, фаза Работен проект.

2.2. Проектните части, свързани с технологията са:

- Част "Конструктивна"
- Част "Електрическа"
- Част "Програмно осигуряване" (софтуер)
- Част "ПБ" (пожарна безопасност)
- Част "ПБЗ" (План за безопасност и здраве)

2.3. Изисквания към съдържанието на разделите на проекта

2.3.1. Част „Конструктивна"

За предвиденото за монтаж ново оборудване (шкафове, мрежови съоръжения или компоненти в шкафовете), да се представят конструктивни чертежи указващи начина на монтаж и укрепване в мястото на монтиране, включително:

- конструкцията на новите шкафове;
- закрепването на оборудването към конструкцията на шкафовете;
- закрепването на шкафовете към съществуващата, строителна конструкция;
- опорна конструкция под шкафовете.

Оборудването на системата за кибератаки трябва да бъде класифицирано като:

- клас по безопасност: 3-Н по НП-001-15;
- категория по сеизмоустойчивост: 3 по НП-031-01.

Размерът на новия шкаф трябва да позволява монтиране на определеното място и да не ограничава достъпа до разположено в близост съществуващо оборудване.

Новото оборудване да бъде със степен на защита в зависимост от групата по пожарна опасност на помещенията, в които се монтират, с цвят RAL 7035 и с надписани технологични наименования. Размерът и цветът на надписите ще се уточни допълнително с Възложителя.

2.3.2. Част „Електрическа”

Електрозахранване

- новото оборудване да не изисква съществена промяна в източниците и схемата на електрозахранване;

- новото оборудване трябва да бъде обезпечено с електрозахранване от два независими канала, за да не може единичен отказ (на захранващ източник или преобразувател на напрежение) да причини загуба на електрозахранване;
- заземяването на новото оборудване трябва да използва наличната, заземителна система в помещението в което ще се монтира;
- активната мощност, консумирана от новодоставеното хардуерно оборудване, трябва да бъде посочена в проектната документация.

Окабеляване:

Всички нови кабели да бъдат ясно маркирани с технологичните обозначения съгласно правилата за присвояване на технологични обозначения в АЕЦ „Козлодуй".

За всички нови кабели трябва да се изготви кабелен журнал, който да съдържа: „Наименование на кабела (марка)", „Начало и край (на всеки кабел)", „Дължина", „Начин на полагане (в различните участъци)", „Тип", „Брой жила" и „Сечение".

Архитектура на системата.

Изпълнителят да представи подробна архитектура на системата за защита от кибератаки.

Хардуерната част на системата за защита от кибератаки трябва да бъде разположена в помещение 5AE128/1 на 5 ЕБ.

Изпълнителят да представи подробен чертеж на новото оборудване и подробен чертеж на инфраструктурния шкаф, със съответните хардуерни компоненти в него.

Изпълнителят да представи подробна архитектура на мрежовите интерфейси на системата за защита от кибератаки, със съответните мрежови устройства.

Изпълнителят да представи пълен списък от съществуващите в информационната система устройствата, към които ще има изградени интерфейси за връзка.

Хардуерно осигуряване:

2.3.2.1. Сървърна конфигурация – минимум четири броя със следните минимални технически параметри:

- Форм фактор-Максимално 1U rack-mount
- Процесор-Инсталирани минимум 2 x Intel Xeon 18C 2,9Ghz 35MB Cache
- Инсталирана оперативна памет-Инсталирана минимум 16 x 32GB ECC DDR4 3200MHz, с включена възможност за допълнителен слой на защита против непланирани прекъсвания
- Поддържана оперативна памет-Минимум 32 слота за памет и 4TB пространство
- RAID контролер-Да поддържа RAID 0,1,5,10,50 и да разполага с 4GB резервирана кеш памет
- Твърди дискове-Инсталирани минимум 2 броя 480GB SSD
- Поддържан брой твърди дискове-Минимум 8 твърди диска SAS/SATA/SSD
- PSU (захранване)-Инсталирани 2 x резервирани захранващи модули минимум 800W Titanium
- LAN-Инсталирани минимум 4 x 10 Gbit SFP+ порта
- Fiber Channel-Да има минимум 2 x 32 Gbit порта
- Портове и слотове-Да разполага с минимум 1 x USB 2.0 и 1 x USB 3.0 преден панел, 2 x USB 3.0 заден панел, 2 x USB 3.0 разположени върху дънната платка, 1 x Display Port преден панел, 3 слота PCIe GEN4 x16, 1 VGA заден панел
- Hot-swap компоненти-Захранващи блокове, охлаждащи модули, твърди дискове
- Поддържани операционни системи-Microsoft Windows Server, RHEL Server, SUSE Linux Enterprise Server, VMware vSphere Hypervisor
- Операционна система-Да бъде доставен с Windows Server Standard 2022, покриващ броя на инсталираните процесорни ядра

- Управление-Да има отделен интерфейс за out-of-band management – 1 отпред и 1 отзад, Wake on LAN, да позволява достъп до сървъра чрез отдалечена конзола и графичен интерфейс
- Гаранция-Минимум 3 години от производителя. Участникът да посочи партиден номер на производителя за поддръжката.

2.3.2.2.Сървъри за бекъп – минимум два броя със следните минимални технически параметри:

- Форм фактор-Максимално 2U rack-mount
- Процесор-Инсталирани минимум 2 x Intel Xeon 8C 3,0Ghz 12MB
- Инсталирана оперативна памет-Инсталирани минимум 4 x 16GB ECC DDR4 3200MHz, с включена възможност за допълнителен слой на защита против непланирани прекъсвания
- Поддържана оперативна памет-Да поддържа минимум 32 слота за памет и 4TB пространство
- RAID контролер-Да поддържа RAID 0,1,5,10,50 и да разполага с 4GB резервирана кеш памет
- Твърди дискове-Инсталирани минимум 2 x 960GB SSD 2.5in.
- Шасито на предложеният сървър да поддържа комбинация от максимум 12 бр. 3,5" дискове и 2 бр. 2,5" дискове
- Поддържан брой твърди дискове-Минимум 8 твърди диска SAS/SATA/SSD
- PSU (захранване)-Инсталирани 2 x резервирани захранващи модули минимум 800W Titanium
- LAN-Инсталирани минимум 2 x 1 Gbit порта и 2 x 10 Gbit SFP+ порта
- Fiber Channel-Да има минимум 2 x 32 Gbit порта
- Портове и слотове-Да разполага с минимум 1 x USB 3.0 преден панел 1x DP на преден панел, 2 x USB 3.0 заден панел, 6 слота PCIe GEN4 x16
- Hot-swap компоненти-Захранващи блокове, охлаждащи модули, твърди дискове
- Поддържани операционни системи-Microsoft Windows Server, RHEL Server, SUSE Linux Enterprise Server, VMware vSphere Hypervisor
- Операционна система-Да се достави с Windows Server 2022 Standard покриващ броя на инсталираните процесорни ядра
- Управление-Да има отделен интерфейс за out-of-band, Wake on LAN, да позволява достъп до сървъра чрез отдалечена конзола и графичен интерфейс
- Гаранция-Минимум 3 години от производителя. Участникът да посочи партиден номер на производителя за поддръжката.

2.3.2.3. SAN комутатори – минимум два броя със следните минимални технически параметри:

- Форм фактор-Максимално 2U rack-mount
- Брой Портове-Минимум 24 броя
- Брой Активни Портове-Минимум 24 броя
- Поддържани скорости на трансфер-Минимум 8/16/32 Gbit FC
- Инсталирани SFP модули и кабели-Да се достави с минимум 10 броя 32Gbit FC и 10 броя OM4 FC 2m кабели.
- Включени софтуерни функционалности-Минимум: Fabric Services, Access Gateway, Fabric Vision, ISL Trunking, Интеграция със системата за съхранение на данни за автоматично дефиниране на зони.
- Инсталация и конфигурация-Да се достави услуга по инсталация и първоначална конфигурация на устройствата от сертифициран специалист.
- Гаранция-Минимум 3 години от производителя. Хардуерна и софтуерна поддръжка от производителя. Участникът да посочи партиден номер на производителя за поддръжката.

2.3.2.4. Дисков масив – минимум един брой със следните минимални технически параметри:

- Форм фактор-Rack-mount – За монтаж в сървърен шкаф
- Архитектура-Архитектура с дублиране на всички компоненти, без единична точка на отказ. Да позволява подмяна/надграждане на всеки един компонент без спиране на работата.
- Контролери-Да се достави с минимум 2 броя с взаимно осигуряване. Всеки контролер да притежава 128GB вградена кеш памет.
- Контролери – Fibre Channel (FC) интерфейс-Системата да разполага с поне 8 броя FC порта със скорост не по-малка от 32Gbps на порт за връзка към мрежата за данни (SAN); Системата да може да се разширява до 16 броя FC порта.
- Поддържани host протоколи от системата - FC, iSCSI
- Капацитет на системата - Предложената конфигурация трябва да съдържа:

  - Минимум 110 еднакви диска 2,4TB 10K SAS
  - Минимум 40 еднакви диска 8TB 7,2K SATA

- Разширяемост на системата-Минимум до 240 броя твърди дискове.
- Поддържани RAID нива-RAID 6
- Производителност (Bandwidth) - Не по-малка от 10GB/s и 26K IOPS
- Функционални възможности на системата-Да бъдат предоставени следните функционалности за целия допустим обем на системата, които покриват:

- свързаност на контролерите към дисковете (backend) – минимум 2бр. четири-канални SAS 12Gb/s порта на контролер.
- Механизъм за защита на данните (RAID protection) или еквивалент;
- Снимка на логически дял от системата (Shapshot);
- Провизиране на виртуално дисково пространство (Thin Provisioning);
- Дедупликация на данните;
- Компресия на данните;
- Възможност за криптиране на данните;
- Приоритизация на услуги (Quality of Service) – включително по времезакъснение.
- Интеграция с доставените SAN комутатори за автоматично дефиниране на SAN зони.
- Синхронна и асинхронна репликация на ниво контролер.
- Функционалност за прозрачно за хостовете преместване на виртуални дискове между 2 системи за съхранение на данни, сертифицирано за VMware. Функционалността да не изисква допълнително оборудване освен арбитър.
- Възможност за разделяне на устройството на виртуални среди с независимо управление и ограничен достъп с цел Multi-tenancy.
- Възможност за управление през облачна конзола.

- Поддържани операционни системи-Минимум: Microsoft Windows Server, HP-UX, Linux, Oracle Solaris, VMware ESXi, Microsoft Hyper-V,
- Управление и наблюдение-Да бъде доставен с включен софтуер за отдалечено и локално управление и наблюдение с GUI/Web и CLI потребителски интерфейс
- Конфигурация на захранващите блокове-Резервирани N+1, сменяеми по време на работа на машината
- Инсталация и конфигурация-Да включва инсталация и първоначална конфигурация на устройствата от сертифициран специалист.
- Гаранция-Минимум 3 години (24 x 7), с време за реакция от момента на уведомяване: до 15 минути за критични инциденти и до 4ч. за посещение на място. Хардуерна и софтуерна

поддръжка от производителя. Участникът да посочи партиден номер на производителя за поддръжката.

2.3.2.5. Софтуер за виртуализация със следните минимални технически функционалности:

- VMware vCenter Server Standard съобразен с избрания хардуер в част „Сървърна конфигурация", с включена поддръжка тип „Production" за 3 години.
- VMware vSphere Hypervisor (ESXi) Enterprise Plus (CPUs) с количество лицензи съобразени с избрания хардуер в част „Сървърна конфигурация", с включена поддръжка тип „Production" за 3 години.

2.3.3. Част „Програмно осигуряване (софтуер)"

Изискваните контролни функции и услуги за сигурност, които трябва да поддържа системата за защита от кибератаки са:

- анализ на събития чрез събиране, наблюдение и анализ на логовете в информационната система или „Security Information and Event Management (SIEM)";
- управление на акаунти и привилегирован достъп;
- реакция, управление и автоматизация на решенията за сигурност или Security Orchestration, Automation & Response (SOAR);
- разузнаване на заплахи;
- киберзащита на крайни точки;
- осигуряване на отдалечен достъп през криптиран канал за комуникация с включени функционалности за инспекция, защита на крайни устройства и VPN без агент (Clientless VPN);

2.3.3.1. Изисквания към функцията - анализ на събития чрез събиране, наблюдение и анализ на логовете в информационната система или „Security Information and Event Management (SIEM)

1. Решението да включва софтуерно решение за анализ на инфраструктурата на Възложителя срещу конвенционални и съвременни сложни киберзаплахи. Решението да включва лицензи за управление на събития и инциденти, свързани със сигурността (Security Information and Event Management - SIEM), оразмерено за обработка на минимум 150GB данни дневно за период от минимум 36 (тридесет и шест) месеца.

2. Решението да бъде доставено в модел за локално (On-prem) внедряване, инсталирано в инфраструктурата на Възложителя.

3. Решението да включва функционалност всички данни за събития в наблюдаваните системи да бъдат съпоставени в един компонент. Всички правила за корелация трябва да се управляват чрез уеб-базиран графичен потребителски интерфейс на системата. Корелацията се състои в установяване на връзки между отделни събития, свързани с киберсигурността.

4. Решението да има единно общо хранилище на данни за всички събрани данни;

5. Решението да има единично търсене или отчет, който може да обхване всички събрани данни;

6. Решението да осигурява уеб-базиран потребителски интерфейс за крайните потребители, без използване на клиент;

7. Решението да разполага с онлайн магазин за допълнителни приложения за различни технологии и разширяване на случаите на употреба;

8. Решението да бъде със скалируема и мащабируема архитектура способна да поеме неограничено съхранение на данни;

9. Решението да може да събира всякакви данни, като съхранява данните в плоски файлове, осигуряващи достъп до всички стойности на данните и полета без схема или

нормализиране;

10. Решението не трябва да налага ограничение на броя полета, които може да индексира;

11. Решението да може да поеме всички оригинални, немодифицирани данни и да ги направи годни за търсене (без намаляване на данните);

12. Решението да може да поставя различни типове данни в различни логически разделени хранилища за данни за оптимална производителност при търсене или за целите на сегрегацията на данни/RBAC;

13. Решението да може да поддържа оригиналните времеви марки за всяко събитие, докато обработва времеви марки от различни часови зони;

14. Решението да включва функционалност за автоматично компресиране на погълнатите данни, за да се намалят изискванията за съхранение;

15. Решението да осигурява гъвкави настройки за съхранение на данни, както следва:

- Настройка за период на съхранение на погълнати данни: дни, месеци или години;
- Настройка/подробен контрол чрез графичния потребителски интерфейс за това какво се случва с данните, когато остареят. Остарелите данни могат да бъдат преместени във външно/по-евтино хранилище и/или изтрити;

16. Решението трябва да поддържа конфигурация за висока наличност и репликация на погълнатите данни, с цел толерантност към бедствия и подобрена производителност при търсене;

17. Решението да включва функционалност за промяна на съществуващите правила за корелация и създаване на нови корелационни търсения;

18. Всяко правило за корелация трябва да има автоматично, конфигурируемо присвояване на тежест, собственик и статус;

19. Правилата за корелация, търсенията и визуализациите трябва да обхващат множество категории и технологии за сигурност, минимум: удостоверявания, използване на акаунти по подразбиране, злонамерен софтуер, промени в крайната точка, нива на корекция, защитни стени, IDS, сканиране за уязвимости, уеб проксита, необичайна HTTP-базирана дейност, и промени в порт/протокол;

20. Решението да включва вградени отчети и табла за управление;

21. Отчетите и таблата за управление трябва да съдържат прости опции за филтриране и полета за формуляри, за да помогнат на потребителите да стеснят данните до това, което ги интересува: Рамка за преглед на инциденти/работен поток за преглед и обработка на инциденти, която трябва да включва подробности за всеки инцидент най-малко:

- Допълнителен контекст от външни източници на активи и самоличност
- Необработените събития, които представляват инцидента
- Историята на работния процес на събитието

22. Таблата и отчетите трябва да се създават лесно за измерване на съответствието с всеки технически контрол, който може да бъде проследен в данните;

23. Таблата и отчетите да могат да се използват за основни разпоредби и рамки, включително:

- PCI
- GLBA
- HIPAA
- FISMA
- SOX

- NERC
- EU Data Directive
- NIST 800-53
- ISO 27002
- COBIT
- SSAE 16

24. Таблата за управление и отчетите трябва да поддържат заявки за вътрешен одит и заявки за одиторска ad hoc информация;

25. Решението да поддържа прилагането на Kill-Chain методология и рамката на MITER ATT&CK за разследване;

26. Решението да включва възможност за ръчна промяна на тежестта на инцидента, състоянието и добавяне на бележки към инцидент;

27. Решението да има възможност за бъдещо надграждане с други случаи на използване като:

- Управление на измами
- ИТ операции
- VMware мониторинг и планиране на капацитета
- Управление на приложения
- Уеб и цифрово разузнаване
- Бизнес анализ
- Индустриални данни и Интернет на нещата

28. Решението да поддържа всякакви източници на данни, включително всяко приложение, ОС, устройство или система, независимо дали са виртуални/физически или базирани на облак;

29. Решението да не разчита на използването на персонализирани конектори за приемане на данни от различни източници;

30. Решението да осигурява възможност за събиране на логове най-малко от следните системи за информационна сигурност:

- Защитни стени
- Система за откриване на проникване / Система за предотвратяване на проникване
- Система за удостоверяване (включително LDAP и Active Directory)
- Предотвратяване на загуба на данни
- Антизловреден софтуер
- Автоматизирани инструменти за анализ на злонамерен софтуер
- Уеб сигурност или уеб прокси
- Защита на имейли
- Скенери за уязвимости
- Мониторинг на целостта на файловете
- Защитни стени за уеб приложения

31. Източници на логове, които не са свързани пряко с киберсигурността трябва да включват най-малко:

- Регистрационни файлове на операционната система (крайни точки и сървъри)
- Имейл сървър
- Уеб сървър
- DHCP/DNS

- VPN
- Мрежови потоци (NetFlow, IPFIX и т.н.)
- PCAP файлове
- Мрежови устройства (рутери, комутатори)
- Бази данни и мейнфрейми
- NAS устройства и файлове
- Хипервайзор и регистрационни файлове на виртуални машини
- Сервизно бюро
- Записи на разговори
- Мобилни устройства и системи за управление на мобилни устройства
- Инструменти за управление на сървъри и крайни точки
- SCADA устройства
- Индустриални системи за контрол
- Производствени системи
- Данни за физически значки
- Хоствани VM среди (Amazon Web Services, Rackspace и т.н.)
- Облачно базирани приложения (Box, Salesforce.com и т.н.)
- Социални медии (Twitter, Facebook, Foursquare и т.н.)
- Уеб анализи
- ERP и CRM
- RFID
- GPS

32. Решението да има възможност за получаване на данни чрез широк набор от механизми, базирани на агенти и без агенти, най-малко чрез:

- Агент, предоставен от производителя. Агентът трябва да има способността да криптира комуникациите към системата, да кешира данните, да балансира натоварването на данните към различни сървъри и да изпраща данните чрез TCP
- Syslog
- TCP или UDP
- SNMP събития
- XML
- CSV
- JSON
- WMI
- Персонализирани входове (Скриптирани входове и модулни входове)

33. Решението да има възможност за директно свързване към всяка таблица на SQL база данни и извличане на съдържанието за поглъщане;

34. Решението трябва да има способността да обогатява по-рано погълнатите данни с външни данни, за да улесни търсенето и отчитането с дни, месеци или години назад;

35. Решението да може да използва необработени погълнати данни за извършване на търсения в база данни или CSV файл:

- Търсените данни да могат да бъдат с всякаква стойност, включително IP адреси, имена на машини или забранени услуги/външни IP адреси/портове/протоколи

36. Решението да поддържа интеграция с корпоративни директории (AD, LDAP и т.н.) за извличане на информация за служители, включително:

- Потребителски имена на служители, име, фамилия, телефон, при възможност ръководен персонал, при възможност структура, местоположение, ако е привилегировано, ако е в списък за наблюдение, начална и крайна дата и т.н.
- Да позволява възможност за свързване на множество потребителски имена към един служител;

37. Решението да поддържа интегриране с CMDB или бази данни за активи за извличане на информация за активи, включително:

- Име на хост на устройството, IP, MAC, местоположение, ако съдържа поверителни данни, ако е уместно за даден регламент и т.н.;
- Да позволява възможност за картографиране на IP към име на машина и обратно;

38. Решението да има възможност за лесно интегриране с безплатни или търговски решения за разузнаване на заплахи на трети страни, четими от човек емисии за разузнаване на заплахи;

39. Решението да има възможност за извършване на пълно текстово търсене във всяко поле в погълнатите данни въз основа на:

- Подобно на Google търсене на ключови думи;
- Избираеми времеви диапазони;
- Конкретни или относителни времеви прозорци до месец/ден/минута/секунда;
- Булева логика (и, или, не и т.н.);
- Регулярни изрази;
- Синтаксис с заместващи символи.

40. Решението да има възможност за извършване на статистически анализ, включително:

- Брой на събитията, различен брой на събитията, сума;
- Най-често срещаните стойности или най-малко често срещаните стойности на поле;
- Минимум, максимум;
- Средно, средно, режим, медиана;
- Стандартно отклонение, дисперсия;
- Идентификация на аномални стойности в резултатите, които може да са нередовни или необичайни;
- Статистическа корелация между полета;
- Групиране на събития заедно въз основа на тяхната прилика едно с друго като едно събитие;
- Съкращаване на извънредни числови стойности в избрани полета, за да подпомогне статистическата корелация;
- Първо и последно видяна стойност;
- Процентил;
- Предсказани стойности (търсене, което разглежда исторически данни, за да предскаже математически бъдещи стойности);
- Извършване на обединение, разлика или пресичане на отделни или множество резултати от търсене;
- Търсене на връзки между двойки полета чрез сравняване на стойностите на едно поле към референтно поле и двойка стойност;

41. Решението да има възможност за извършване на базова линия и след това прилагане на горната логика на търсене, за да се намерят отклонения/аномалии от базовата линия, които

може да са напреднали, не базирани на сигнатура заплахи;

42. Търсенията да могат лесно да се запазват, споделят и променят;

43. Търсенията да могат да бъдат в реално време или по график;

44. Решението да има възможност за извършване на множество едновременни търсения;

45. Решението да има следните възможности за известяване в реално време на базата дефинирано търсене:

- Изпращане на имейл;
- Добавяне към RSS емисия;
- Изпълнение на готови действия на защитни стени, системи за предотвратяване на проникване и сигурност на крайната точка;
- Изпълнение на персонализиран скрипт;
- Скриптове действащи като „среден софтуер“ позволяващи автоматизирани действия за справяне със заплаха;

46. Решението да няма фиксиран максимален брой търсения или сигнали, които могат да бъдат стартирани;

47. Решението да позволява създаване на широк набор от визуализации (не ограничени до фиксирани, предварително консервирани отчети), Визуализациите трябва да включват:

- Таблици
- Времеви диаграми
- Линейни диаграми
- Стълбовидни диаграми
- Диаграми с площи
- Кръгови диаграми
- Точкови диаграми
- Радиални, пълнители и маркери
- Карти

48. Визуализациите да имат възможност за актуализиране в реално време;

49. Визуализациите да могат да показват отклонения/аномалии, които се нуждаят от допълнително изследване;

50. Визуализациите да поддържат възможности за детайлизиране, кликване за достигане на резюмета до необработени събития в рамките на секунди;

51. Да има възможност за конвертиране на табла за управление в PDF файлове и планиране на изпращането им по имейл до други;

52. Да има възможност за интегриране с външни рамки за визуализация и опции (D3, Tableau и т.н.) за допълнителни визуализации;

53. Решението да има гъвкав контрол на достъпа, базиран на роли за контролиран потребителски и API достъп. Да позволява ограничен достъп до конкретни източници на данни, типове данни, периоди от време, конкретни изгледи, отчети или табла за управление;

54. Решението да има възможност за интегриране на удостоверяване и оторизация с Microsoft Active Directory, Novell eDirectory и други LDAP-съвместими реализации;

55. Решението да има възможност за интегриране към корпоративни решения за единично влизане, позволяващи преминаващо удостоверяване на идентификационни данни на трети страни;

56. Решението да наблюдава собствените си конфигурации и използване, за да поддържа пълна, цифрово подписана одитна пътека за това кой има достъп до системата, какви търсения изпълнява, какви отчети преглежда и какви промени в конфигурацията прави;

57. Решението да предлага готови API за излагане на всички погълнати данни, команди

за търсене и функционалност на външни системи, приложения или табла за управление;

58. Решението да предлага готови документирани SDK за програмен достъп до системната конфигурация и извличане на данни;

59. Всички системни конфигурации трябва да могат да се конфигурират чрез потребителския интерфейс или CLI, което позволява детайлни промени и персонализиране;

60. Решението да предлага възможност за препращане на данни към външни системи или инструменти за регистриране;

61. Решението трябва да бъде инсталирано върху сървър/и предоставен/и от Изпълнителя като част от системата. Решението трябва да бъде инсталирано върху минимум 4 броя виртуални машини с операционна система 64-bit Linux или Windows дистрибуция, които е допустимо да бъдат върху един физически сървър със следните минимални параметри:

- Минимум 64 физически ядра;
- Минимум 256GB оперативна памет (RAM Memory);
- Общо дисково пространство – минимум 15TB SSD.

62. Предложеното решение да включва право за ползване за период не по-малък от 36 месеца.

2.3.3.2. Изискване към функцията - управление на акаунти и привилегирован достъп

1. Да се достави софтуерно решение за управление и защита на привилегировани потребители и акаунти с включени всички необходими лицензи с права за ползване на всички изисквани функционалности за 20 (двадесет) администратора на Възложителя;

2. Решението да включва функционалност за управление и защита на привилегировани потребители и акаунти (автоматична промяна на пароли, определяне на политиката за достъп) в следните системи наричани по-долу "целева/целеви система/и":

- Операционни системи: Windows, Unix, Linux, iSeries (AS / 400), zSeries (OS / 390)
- Бази данни: Microsoft SQL, Microsoft SQL Cluster Service, Oracle, Informix, MySQL, Sybase Adaptive Server Enterprise, HeidiSQL, DB2, Informatica, MariaBD, MongoDB, PostgreSQL
- Системи за управление на инфраструктура и приложения: DELL DRAC, IBM Tivoli, RSA мениджър за удостоверяване, HP iLO, SAP Application Server
- Мрежови устройства и системи за сигурност: Cisco (рутери, Nexus серия, защитни стени), HP, Checkpoint, Netscreen, F5, Infoblox NIOS, FireEye Malware Analysis, FortiGate, Aruba, Palo Alto Networks, A10, Riverbed, Thales
- CI/CD инструменти: Chef, Jenkins, Kubernetes, Docker
- Модули: Майкрософт услуги, планирани задачи, Microsoft IIS, в регистрите, COM +, управление на акаунти в домейна на Microsoft
- Пароли запазени в конфигурационни файлове, таблици на бази данни
- VMWare ESX / ESXi среда за виртуализация, vCenter

Системата трябва да включва функционалност за управление на привилегировани акаунти за системи извън посочените по-горе, използвайки скриптове или други механизми, внедрени и поддържани от производителя на решението за промяна на парола чрез: SSH / Telnet, API за външни приложения;

3. Решението да включва функционалност за защита на акаунта и автоматична ротация на паролата за всяко устройство, което поддържа ODBC версия 2.7 или по-висока;

4. Решението да включва функционалност за управление на привилегировани потребители и акаунти, използвани в целевата система под формата на предефинирани списъци чрез използването на скриптове или други механизми на имплементация за целеви системи като: Cisco, Microsoft Windows, Microsoft SQL, Linux / Unix, Oracle, MySQL, VMWare, AS400,

OS390, DB2, SAP

5. Решението да включва функционалност за автоматично откриване на привилегировани акаунти в нови устройства с Windows, услуги на Windows, планирани задачи (Scheduled Tasks), акаунти за IIS услуги и др., Автоматично да добавя горните акаунти към системата и автоматично да прилага подходяща политика за управление на привилегированите акаунти;

6. Решението да включва функционалност за защита на акаунта и динамично да генерира нов SSH ключ, в съответствие с посочен шаблон;

7. Решението да включва функционалност да валидира паролите/SSH ключовете, които съхранява в дигиталния сейф с паролите/SSH ключовете съхранени на целевата система съгласно дефинираната политика;

8. Решението да включва функционалност за автоматично синхронизиране на паролите/SSH ключовете, съхранявани в дигиталният сейф и паролите/SSH ключовете, съхранявани в целевата система в случай на несъответствие.

9. Решението да включва функционалност за съхраняване на историята на промяна на паролите (например последните три пароли за дадена целева система) и да позволява лесен достъп до тази история (например чрез уеб интерфейс);

10. Решението да включва поддръжка на различни LDAP среди за удостоверяване на потребителя, за Sun One, Microsoft Active Directory, IBM Tivoli, Novel eDirectory, Oracle Internet Directory;

11. Решението да включва функционалност за откриване на двойки SSH ключове в инфраструктурата;

12. Решението да включва функционалност за управление по сигурен начин на SSH ключове използвани от приложения в конфигурационните файлове;

13. Решението да включва функционалност за изолиране, наблюдение и запис на сесиите без да разкрива паролите на привилегированите акаунти на клиентската машина. Когато потребителят е разпознат по сигурен начин и привилегированият акаунт е разрешен, предложеното решение автоматично да взема привилегированите пароли от дигитален сейф, да стартира избраното от потребителя приложение (приложението да е инсталирано предварително) и да предостави паролата в приложението без да я дистрибутира на работната станция на потребителят. Записът на сесиите с индексирането на данните да е налично като възможност за конфигурация на ниво политика;

14. Решението да включва функционалност по сигурен начин да установи и управлява привилегировани сесии (Не се допуска предложеното решение да установява сесии до системите посочени по-долу посредством допълнителни „jump hosts“/„bastion hosts“, до които потребителят може да достигне, да избере апликация и ръчно да вкара паролите), за не по-малко от долните системи:

- Операционни системи: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390)
- Бази данни: Microsoft SQL, Oracle, MySQL, SAP HANA, HeidiSQL, DB2
- Системи за управление на инфраструктурата и приложения: DELL DRAC, RSA authentication Manager, HP iLO, SAP GUI, BMC Remedy
- Мрежови устройства и такива свързани със сигурността: Cisco (routers, nexus switches, firewalls)
- CI/CD tools (https, ssh): Chef, Jenkins, Kubernetes, Docker, Jfrog, GitHub
- Виртуализация: VMWare ESX/ESXi, vCenter (vSphere Client, https, ssh)

Да се поддържа функционалността на Microsoft Remote App за публикуване на приложения. Системата да включва предоставени от производителя скриптове за подобряване на сигурността на операционната система, които да бъдат изпълнени по време на инсталация.

15. Решението да включва функционалност за наблюдение и разделяне на сесии и изпълнение на функция за единно влизане (Single Sign-On) за привилегировани акаунти и за други приложения и системи, различни от посочените в горната точка, чрез не по-малко от следните възможности: стартиране на приложението със специфичен набор от параметри, използвайки скрипт, вграден компонент за поддръжка за управлението на клиентски уеб приложения;

16. Решението да включва функционалност да съхранява записи на сесии на криптирано хранилище, което да ги предпазва от манипулиране. Никой от потребителите, включително Системният администратор да не е в състояние да засегне интегритета на съхраняваните записи (включително невъзможност за триене по време на дефинирания период на съхранение);

17. Решението да включва функционалност за управление на достъпа до целеви системи и създаване на списък от разрешени и забранени команди изпълнени през SSH;

18. Решението да включва функционалност гарантираща отчетност в случай на използване на споделени акаунти от повече от един потребител по едно и също време;

19. Решението да използва механизъм за индексиране на метаданни (в записа на сесии), за да извършва бързо търсене в записаните и мониторирани сесии, чрез специфични думи и активности (трябва да се поддържат следните индексиращи механизми като минимум: натиснати клавиши, отговор от Win OS, SQL команди). Не е допустимо предложеното решение да идентифицира метаданни чрез OCR (оптично разпознаване);

20. Решението да включва функционалност за потребителски достъп до защитените ресурси с поддържане на следните инструменти/методи като минимум:

- уеб интерфейс за управление;
- различни RDP клиенти, използвани на работната станция от която се извършва привилегирования достъп, но не по-малко от: дефиниране параметрите на връзката в рамките на RDP конфигурационния файл на клиента или интерактивно питане до потребителя за настройките на защитените системи (като адрес, клиент, приложение, име на привилегирования акаунт). Системата да поддържа PKI сертификати като метод да се автентикира директно до модула за разделяне на сесиите;
- Уеб браузър, който поддържа HTML5 за осигуряване на сигурен потребителски достъп за операционни системи различни от Windows (без RDP клиент); Привилегированата сесия да бъде тунелирана в html5 и налична за потребителя като нов таб в браузъра;
- Различни command line и SSH клиенти (напр. Putty), с автентификация на системата базирана на SSH ключове;"

21. Решението да включва функционалност крайният потребител да избира дали специфична графична сесия да се установи през RDP протокол или HTTPS (сесия тунелирана в HTML5, на база изискванията в горната точка);

22. Решението да включва функционалност да предоставя времеви ограничен привилегирован достъп след одобрение на необходимото искане от оторизиран служител. Разрешенията за времеви достъп трябва да се изключват автоматично след надвишаване на одобрената времева рамка на ескалирани привилегии;

23. Решението да включва функционалност да предоставя времеви ограничен привилегирован достъп до всички целеви системи;

24. Решението да включва функционалност за трансфер на файлове и клипборд за HTML5 тунелираните сесии;

25. Решението да включва функционалност да категоризира записаните потребителски сесии на база риск. Рискът да може да бъде дефиниран в конфигурацията от системния администратор в зависимост от набора функции или команди, открити по време на сесията, и теглото, което им е възложено. Рискът да бъде оценяван по време на текущите сесии.

Информацията за нивото на риск от сесията да бъде видима в конзолата за мониторинг на сесията и в интерфейс показващ инциденти с риск. Администраторът да може да дефинира в резултат на кои действия, извършени от потребителя, сесията да бъде автоматично прекратена;

26. Решението да включва вградени аналитични инструменти, позволяващи автоматично (без външна намеса и необходимост да се определят правила за политика на сигурност) откриване на подозрителна активност на привилегировани акаунти въз основа на автоматично научени потребителски модели (стандартно работно време, IP адреси, брой препратки към дигиталния сейф за пароли и акаунти);

27. Решението да включва функционалност да събира данни за потребителска активност от външни SIEM системи, като поддържа минимум следните решения: Arcsight, Qradar, Splunk, LogRhythm, RSA, McAfee. Да е възможно подаването на информация към SIEM система за аномалии на използването на привилегировани акаунти, открити с помощта на адаптивни алгоритми на следене поведението на потребителите;

28. Решението да включва функционалност да предприема активно действие (като минимум да изисква промяна на привилегирована парола) в случай на аномалии при използването на привилегировани акаунти (кражба на паролата на привилегирован акаунт или създаване на нов акаунт и опит за свързване със сървъра);

29. Решението да включва функционалност да генерира аларма в случай на откриване на прекомерно използване на привилегировани акаунти от даден потребител и в случай на използване на привилегирован акаунт в нестандартни часове (например извън типично работно време за даден потребител);

30. Решението да включва функционалност да открива инциденти, включващи директен достъп на потребителя до целева система (например без предварителна заявка за парола към целевата система), създавайки в целевата система неуправляем привилегирован акаунт. Решението да реагира на този вид дейност чрез налагане на промяна на паролата на новосъздадения привилегирования акаунт в целевата система, добавяне на новосъздадения акаунт в дигиталния сейф и автоматична смяна на паролата;

31. Решението да включва функционалност за одитиране и мониторинг на текуща сесия, спиране/терминиране на сесии, дефиниране на група от събития (команди, стартиране на приложения и др.), за които системата трябва автоматично да терминира сесия;

32. Решението да включва функционалност за инсталиране на базата данни на дигитален сейф на отделна, сигурна OS която да не бъде споделена с другите модули като: прокси за изолация на сесиите, модул за уеб интерфейс, модул за аналитика, модул за периодична промяна на паролите;

33. Изпълнителят да предостави процедури разписани от производителя на предложеното решение, описващи метода за подсигуряване на допълнителна защита на всеки от системните компоненти и да предостави скриптове за автоматизация на процеса в рамките на инсталационните пакети на решението, адаптирани за всеки от отделните модулите. Защитата на всеки компонент трябва да се извърши съгласно добрите практики на производителя на операционната система и на предложеното решение. Защитата на операционната система на дигиталния сейф за пароли да бъде направена автоматично от инструмента за инсталация на предложеното решение по време на процеса по имплементация;

34. Предлаганото решение трябва да включва лицензи за не по-малко от един дигитален сейф с възможност за създаване на 4 резервни копия в режим отказоустойчивост или възстановяване при бедствие и 5 модула за промени и управление на ключове и пароли в защитени системи.

35. Решението да включва права за ползване на неограничен брой модули за изолация на сесиите и наблюдението, също така и неограничен брои модули за уеб потребителски интерфейс на решението (добавянето на допълнителни модули да не изисква закупуването на допълнителни лицензи/абонаменти от производителя);

36. Решението да включва функционалност за имплементиране на дигитални сейфове в дистрибутирана форма, както следва: един основен активен дигитален сейф, един резервиран дигитален сейф в режим възстановяване при бедствие и набор от активни географски дистрибутирани дигитални сейфове, осигуряващи (в режим на четене) най-критичните функции за крайните потребители (например механизъм за резервни копия, споделяйки данни за привилегированите акаунти с приложения, достъп до потребителския интерфейс, установяване на привилегировани сесии по сигурен начин). Предложеното решение трябва да поддържа не по-малко от 5 активни хранилища на идентификационни данни (дигитални сейфове). Цялата система да се управлява от централен графичен интерфейс;

37. Решението да поддържа дистрибутирана архитектура, в която отделните функционални модули (прокси, модул за ротация на паролите, WebUI интерфейс) са инсталирани на множество локации (географски разделени) и комуникират с дигиталния сейф, използвайки сигурен комуникационен протокол (работещ на един от TCP портовете, който да бъде обявен по време на инсталацията). В случай на дистрибутирана архитектура цялата система трябва да се управлява от централен графичен интерфейс;

38. Осигуряването на непрекъсваемост на работата на дигиталния сейф да бъде реализиран на слоя на предложения софтуер, а не на операционната система, на която е инсталиран софтуерът;

39. Решението да включва функционалност за криптографска защита на резервните копия генерирани от продукта;

40. Решението да включва функционалност за интегриране със системи за известяване на кейсове като: BMC Remedy, ServiceNow и други чрез отворен API;

41. Решението да поддържа интеграция с HSM решения, поддържащи стандарта PKCS11, като Atos HSM TrustWay Proteccio, Gemalto Luna / Safenet 1700 хардуерен модул за сигурност, Thales nShield Hardware Security Module, Utimaco CryptoServer;

42. Решението да включва функционалност за интегриране с механизмите, използвани за удостоверяване на потребителя, като минимум парола, LDAP, Windows NTLM, PKI, RADIUS, SAML, многофакторна автентификация, RSA SecurID, Oracle , Amazon Cognito Authentication, OpenID Connect (OIDC);

43. Решението да включва официалната методология за имплементация налична на сайта на производителя. Методологията трябва да покрие описание на главните стъпки, които да се предприемат, за цялостна и изчерпателна имплементация на решението;

44. Решението да включва подсистема за мулти фактор автентификация и предоставяне на сигурен отдалечен достъп за привилегировани потребители;

45. Решението да включва функционалност за:

- адаптивна мултифакторна автентификация
- защита на достъпа до: вътрешни и външни приложения (SaaS), чрез предоставянето на сигурен SSO портал

46. Решението да включва следните методи за мултифакторна автентификация, като минимум: парола, SMS, e-mail, OAuth, (генериран като част от процеса по автентификация на системния интерфейс, осигуряващ автентификация на потребителя през мобилна апликация, вече регистрирана в системата);

47. Решението да включва функционалност за контекстуална информация на база: IP адрес, ден от седмицата, дата, диапазон от дати, времеви диапазон. Решението да включва адаптивна MFA с анализ на потребителското поведение (на база профил на устройството, IP адрес);

48. Решението да включва функционалност за мултифакторна автентификация за решения за VPN (минимум: Cisco Systems, Palo Alto Networks, Fortinet, Juniper) през Radius

протокол;

49. Функционалността за мултифакторна автентификация да се достави като външна услуга (SaaS) с отделни модули/ (конектори) за инсталиране в средата на клиента за интеграция с AD / LDAP система и да осигури Radius сървър интерфейс за мрежовата среда;

50. Решението да включва функционалност за интеграция с различни приложения, които се нуждаят от защита. Системата да предлага следните интеграции като минимум:

- Browser plugin
- NTLM
- Basic auth
- Client Oauth2
- Server Oauth2
- OpenID Connect
- Saml
- User-password

51. Решението да включва интеграция с минимум следните апликации: Adobe Sign, Amazon Web Services, Box, Dropbox, NetSuite, Office 365, Salesforce, ServiceNow, Slack, Webex, Zendesk.

52. Решението да включва функционалност за установяване на сигурна връзка без нужда да се настройва допълнителен VPN тунел между работна станция на потребителя и центъра за данни при нужда от достъп на външни потребители към уеб приложението в локалния център за данни;

53. Решението да включва функционалност за осигуряване на сигурен привилегирован отдалечен достъп на партньори и външни организации без нуждата от VPN (нито site-to-site, нито client-site);

54. Решението да включва функционалност на работните станции да не се инсталира допълнителен софтуер, освен браузър. Решението трябва да поддържа следните браузъри като минимум: Edge, Chrome, Internet Explorer, Firefox;

55. Решението да има архитектура позволяваща установяване на криптирана връзка между работни станции на 3-ти страни/партньори и мрежата на организацията, без нужда от отваряне на портове за входящ трафик до мрежата на организацията. За целта решението да е базирано на SaaS приложение (налично в региона на EU), за да установи трафик от 3-ти страни/партньори и трафик от клиентската среда. SaaS приложението трябва да съдържа функционалност администратора да разрешава достъп на 3-ти страни (лицето отговорно за поканата на 3-тата страна трябва да може да генерира, приеме и автоматично да изпрати съобщения до е-мейл адресите предоставени по време на регистрацията). SaaS приложението трябва да предостави възможности за управление на потребителите (създаване на нови покани, одобряване, деактивиране на акаунти). Достъпът до SaaS приложението да се контролира на база сигурна биометрична автентификация, без нуждата да се предоставят потребителските данни за достъп (като име, или парола);

56. Решението да включва функционалност за биометрична автентификация (на база пръстов отпечатък, smartphone face ID) като начин да се автентифицират 3-ти страни (без нужда да се достъпват данните за достъп, като потребител - парола, преди установяване на връзката);

57. Решението да поддържа не по-малко от следните OS за телефони: IOS версия 17 и по-висока, Android версия 11 и по-висока. Биометричните данни трябва да се съхраняват в Secure Enclave/Trusted Execution Environment;

58. Решението да включва функционалност мобилната апликация която допълнително да предлага функция за одобрение за ключови операции извършвани от SaaS приложението, като даване на административни права на други потребители;

59. Решението да включва функционалност за RDP тунелиране през HTML5 и SDP протокол;

60. Решението да включва функционалност за трансфер на файлове по време на графична сесия;

61. Решението да включва REST API интерфейс за автоматизиране на процеса по управление на потребителите;

62. Мобилната апликация на решението да включва функционалност за изпращане на покана до други потребители. Процесът трябва да включва автоматично създаване на идентичност на външен потребител в платформата за управление на акаунти и привилегирован достъп;

63. Решението за управление на акаунти и привилегирован достъп и подсистемата за мулти фактор автентификация и предоставяне на сигурен отдалечен достъп да бъдат интегрирани помежду си.

64. Предложеното решение да включва право за ползване за период не по-малък от 36 месеца.

2.3.3.3. Изискване към функцията - реакция, управление и автоматизация на решенията за сигурност или Security Orchestration, Automation & Response (SOAR)

1. Решението да предоставя автоматичен отговор на инциденти по сигурност;

2. Решението да предоставя интерактивно разследване на инциденти, сътрудничество между отделните екипи и анализатори, документиране и исторически преглед на извършените действия;

3. Автоматизацията в решението да бъде реализирана чрез използването на модулен модел за изграждане процеси и скриптове;

4. Всяка автоматизация (Playbook) да бъде визуализирана в графичния интерфейс като диаграма изградени от отделни процеси с възможност да се редактира;

5. Решението да поддържа скриптинг реализиран чрез Python и JavaScript както и да предоставя възможност за изтегляне на Python библиотеки с цел преизползване;

6. Решението да предоставя автоматизация и интеграция със следните системи:

- Система за Malware Prevention & Forensic;
- Система за комуникация и кореспонденция;
- Система за SIEM (двупосочна интеграция);
- Система за защита на крайно клиентските машини;
- Мрежова сигурност и защитни стени (двупосочна интеграция);
- Система за откриване на интелигентни заплахи и мониторинг (Thread Intelligence);
- Активна директория

7. Интеграцията с активната директория да се осъществява чрез двупосочен API като системата да може да изтегля информация за потребители, машини, изтекли пароли и информация за групи към които принадлежат тези потребителите;

8. Решението да може да се интегрира двупосочно чрез API с предложената система за анализ на потребителското поведение чрез събиране, наблюдение и анализ на логовете в корпоративна мрежа или „Security Information and Event Management (SIEM)";

9. Решението да може да се интегрира с имейл като позволява слушане и изпращане на имейл към крайните потребители;

10. Решението да може да чете имейл комуникация и да използва получената информация за изпълнение на задачи, одобрение, обратна връзка от потребител или аналитик;

11. Решението да има предефинирани автоматизирани книги за решение на комплексни проблеми;

12. Решението да има възможност да бъде обогатяване с допълнителни автоматизирани книги с отворен код чрез GitHub като всички книги се публикуват и одобряват след верификация от екип на производителя;

13. Решението да позволява на Възложителя сам да създава автоматизирани книги като използва съществуващи или стартира от начало;

14. Автоматизирани книги трябва да може да се създават през графичния интерфейс на системата;

15. Автоматизираната книга да предоставя възможност да включва ръчни задачи, автоматизирани задачи, филтри, други книги, събиране на информация и задачи с условие;

16. Решението трябва да може да стартира автоматична книга при регистриране на инцидент в системата и/или като регулярна задача реализирана на определен период от време;

17. Изпълнението на автоматизирана книга и нейния резултат трябва да бъде напълно документирано като за всеки инцидент има напълно отделно събитие;

18. Анализатора да има възможност да контролира и стартира автоматизирана книга от точка в която автоматизацията е спряла поради очакване на входна информация, проверка на резултат и потвърждение или грешка;

19. Решението да може да рестартира автоматизирана книга в случай, че дадена задача не бъде изпълнена поради грешка;

20. Решението да разполага с възможност за различни права за достъп до нея на база на роли от активна директория;

21. Решението да може да създава автоматизирани книги при които автоматизация да изчаква потвърждение или въвеждане на допълнителна информация от анализатор или управляваш служител (execute users);

22. Решението да притежава API интерфейс, WEB интерфейс, CLI интерфейс и да разполага с мобилно приложение (налично за iOS и Android);

23. Решението да разполага с модул „War Room" за управление на киберкризи, в който всички анализатори да могат да си сътрудничат в реално време, да изпълняват команди и с възможност за известяване през система за кратки съобщения (примерно Slack);

24. Решението да предоставя двупосочна интеграция със системи за управление на инциденти (Jira, RSA Archer, ServiceNow, HP Service Manager, Remedy), като потребителите да могат да създават, търсят и обновяват тикети с информация от разследването;

25. Решението да подържа екипи от анализатори като даден инцидент да може да бъде насочен към екип от анализатори притежаващи една и съща роля;

26. Решението да предоставя възможност за настройка на SLA с който да се измерва производителността и времето за решение на даден инцидент;

27. Анализатора трябва да има възможност и/или да бъде задължен да попълни форма с данни преди да затвори дадения инцидент;

28. Инцидентите в системата трябва да могат да се създават автоматично или ръчно като се използва интеграция с външни системи чрез REST API;

29. Решението трябва да може на база на входящи данни и машинни данни (Machine learning) да открива еднакви инциденти (дублирани). По този начин анализатора да може да проследява как даден инцидент е решен и да се обучава какви са следващите стъпки за най-бързо решение;

30. Решението да може да събира и обобщава данни за минало разследване на даден „тикет" като коментари, източници на данни, име на анализатора работещ по „тикета".

31. Инцидентите да може да се документират автоматизирано като се създава детайлен отчет на всички стъпки предприети по време на разследването;

32. Решението да документира всички промени по инцидента, екип и анализатор, свършени задачи, интерактивни команди, доказателства, чат, записки, задачи изпълнени от автоматизирани книги;

33. Анализаторите да има възможност да комуникират през системата (чат) с цел по бързо решение на инцидента.

34. Решението да има възможност да извършва двустранна корелация между инциденти и индикатори. Анализатора да може да вижда всички индикатори към даден инцидент и обратно;

35. Решението да предоставя възможност за допълнителна интеграция или редактиране на съществуваща чрез PyCharm или аналогичен продукт базиран на Python;

36. Решението да предлага минимум 850 или повече различни интеграции и минимум 1000 или повече автоматизирани книги;

37. Решението да бъде инсталирано в сървърно помещение (център за данни) на Възложителя (on-prem);

38. Решението да се лицензира на брой анализатори, като Изпълнителят предлага всички необходими лицензи за едновременната работа на 3 анализатора и 2 одитора;

39. Решението да има модулна архитектура като да има възможност за инсталация на допълнителни модули в изолирани и отдалечени мрежи с цел предоставяне на защитен достъп до цялата инфраструктура;

40. Решението трябва да позволява на потребителите да създават нови типове IOC и инциденти, които включват дефинирани от потребителя параметри;

41. Решението трябва да има възможности за търсене, които да позволяват на потребителите да търсят информация, индикатори и други подходящи полета от минали случаи/инциденти;

42. Решението трябва да поддържа собствени мобилни клиенти на iOS и Android, за да могат потребителите да постигнат надзор на инциденти с един поглед, както и да предприемат действия или да предоставят необходимата информация;

43. Решението трябва да има вградена поддръжка за различни структурирани формати на Threat Intelligence (най-малко JSON, CSV, STIX 1.x и STIX 2.x);

44. В допълнение към гореописаните задължителни формати за емисии решението трябва да има вградена поддръжка за поне някои неструктурирани формати като електронна поща, новини, RSS канали и други подобни;

45. Решението трябва да позволява автоматично премахване на дублирането на индикатори;

46. Решението трябва да поддържа RBAC (контрол на достъпа, базиран на роли), който да бъде посочен за всяка автоматизация, за да се гарантира, че само оторизирани потребители имат право да ги изпълняват;

47. Решението трябва да бъде инсталирано върху специализиран сървър предоставен от Изпълнителя като част от Системата;

48. Предложеното решение да включва право за ползване за период не по-малък от 36 месеца.

2.3.3.4. Изискване към функцията - разузнаване на заплахи

1. Решението да включва разузнаване за заплахи на база отворени (уебсайтове, paste sites, хранилища за код (code repositories)) и затворени източници (TOR сайтове, форуми със силно ограничен достъп в darknet, пазари в darknet). Технически източници, включително сайтове за анализ на зловреден софтуер и индикатори на заплахи;

2. Решението да предоставя данни от трети страни - минимум Reversinglabs, Shodan, Avast, URLscan, като служи за единствен източник за получаване на разузнавателна информация за заплахи;

3. Решението да предоставя информация за заплахи от доставчици като VISA и различни ISAC групи;

4. Решението да има достъп да събира и предоставя информация зя заплахи от високи

нива на руски, китайски и бразилски криминални форуми;

5. Решението да събира и предоставя данни от затворени общности в тъмната мрежа и да предоставя опционални услуги за взаимодействие с участници в тъмната мрежа от форуми от средно и високо ниво, които имат следните характеристики:

- Реномиран ESCROW процес;
- Задължителен и взискателен процес на проверка за достъп.

6. Решението да извършва активно наблюдение на ботнет мрежи и да предоставя възможност за подробни репорти;

7. Разузнавателните данни в решението, предоставени й от трети страни да бъдат допълнително обогатени с информация и потвърдени;

8. Решението да използва "Natural Language Processing" за автоматизирано анализиране на текст от различни езици, минимум: арабски, китайски (както опростена, така и традиционна писменост) английски, фарси (персийски), френски, немски, италиански, японски, португалски, руски, испански, шведски;

9. Решението да е достъпно през единен портал, посредством уеб браузър, като уеб съдържание или чрез API като JSON или през TAXII CVS-STIX формат. Информация или визуализации от платформата да могат да бъдат експортирани във формати: JSON, CSV, STIX, PPT, PNG, PDF и Word документи;

10. Достъпът до различни функционалности/информация в решението да бъде разделен на модули с възможност за конфигуриране на ролеви базиран достъп;

11. Решението да е защитено с мерки за информационна сигурност като:

- Шифрирани и хеширани пароли;
- Активно смекчаване на DDoS;
- Автоматично блокиране на акаунти;
- Обширен контрол на достъпа до съоръженията на производителя;
- Многофакторна автентификация;
- Цялостна програма за разузнаване на заплахи;
- Автоматизирани сканирания за сигурност на обслужващите системи;
- Тестване за активно проникване;
- Обширна програма за информираност и обучение за вътрешна сигурност за служителите;
- Записана програма за докладване на бъдещи уязвимости;
- Специален екип за сигурност на продуктите, който претърсва платформата за потенциални уязвимости и помага на инженерите да доставят защитен код;

12. Решението да се обновява с нови данни в реално време;

13. Решението да разполага и предоставя исторически данни за заплахи минимум 10 години назад;

14. Наблюдението на тъмната мрежа да бъде постигнато посредством автоматизирани и ръчни методи за активно наблюдение. Решението да използва алгоритми за машинно обучение за събиране, структуриране и анализиране на данни със скоростта и мащаба на интернет, както и да използва ръчно събиране, което да се извършва от членове на вътрешен екип за изследване на заплахите;

15. Решението да включва функционалност за засичане на Domain Abuse, като наблюдава и събира информация от издателите на сертификати с фокус в/у домейни видени за първи път в Certificate Trust List. Подхода да позволява разширяване на информацията за поддомейни и напълно квалифицирани имена на домейни (FQDN), както и за домейни от най-високо ниво (TLD), които имат регистратори, които са ориентирани към поверителността или са секретни;

16. Решението да открива и алармира за възможно имитиране на фирмени ръководители,

уебсайтове, домейни и лога;

17. Решението да открива и алармира за изтичане на лична информация, като имейл адреси и пароли;

18. Решението да открива и алармира нарушение на търговската марка;

19. Решението да предоставя оценка на риска за различни URL-и;

20. Решението да може да идентифицира измами с ваучери и злоупотреба с ваучери;

21. Решението да засича "typosquat" домейни от поне 20 различни типа DNS-Twist правила;

22. Решението да открива компрометирани креденшъли онлайн;

23. Възложителят при нужда да има възможност да заяви срещу допълнително заплащане следните допълнителни услуги към производителя за сваляне на съдържание:

- Домейни/уеб сайтове с подобен URL адрес на марката , който хоства злонамерено или phishing съдържание.
- Domain squats;
- Злоупотреба с марката в социалните медии. Представяне на марката напр. Twitter профил използващ брандинг (лого) на организацията, туитващи връзки към измама с криптовалута.
- Измамно съдържание или съдържание в нарушение на марката. Това може да се състои от фалшиви обяви за работа или фалшива връзка с клиент.
- Неоторизирани мобилни приложения. Мобилни приложения, използващи брандиране на организцията без разрешение; например дублиране на легитимно приложение или версия, която е била подправена (рекламен, злонамерен софтуер, шпионски софтуер и т.н., вградени в приложението, създавайки негативно изживяване за крайния потребител и причинявайки щети на марката).
- Сървъри за злонамерен софтуер, насочени към клиенти. Изпускане на зони, командни и контролни структури, пренасочвания на зловреден софтуер и изтегляния.

24. Решението да включва sandbox функционалност, като отчетите да могат да се предоставят в JSON формат. Пробите обработени от sandbox да се съпоставят с техниките на MITRE ATT&CK;

25. Решението да предоставя оценки на риска в реално време, базирани на доказателства и видимост в/у правилата които образуват оценката на риска, както и тяхното подробно описание;

26. Решението да предоставя контекст, свързан с IOC-та (Indicators of Compromise) напр. връзки към участници в заплахата, методи за атака и други;

27. Решението да предоставя данни за IOC, минимум: IP адреси, URL адреси, домейни, хешове/имена на файлове;

28. Предоставяните данни да могат да доставени в машинно четим и стандартизиран формат, като STIX/TAXII.

29. Решението да притежава RESTful JSON API;

30. Решението да предлага възможност за бъдещо надграждане с интеграции с различни SIEM решения, минимум с предложеното от Изпълнителя SIEM решение. Интеграциите на платформата да позволяват на потребителите да получават обогатени данни за IOC директно в SIEM системата;

31. Решението да поддържа интеграция минимум с предложената SOAR система, както и Siemplify, Phantom, XSOAR, като да поддържа следните сценарии:

- Обогатяване - автоматизиране на процеса на извличане на външни данни за риска и контекст на indicator of Compromise (IOC);

- Корелация - идентифициране и корелация на връзки между логове на корпоративни системи и външната информация за риска;
- Мониторинг - алармиране за специфични за организацията субекти, открити при разузнаването на външни заплахи.
- Лов на заплахи - проактивно и интерактивно търсене в мрежи за откриване и изолиране на напреднали заплахи, които избягват съществуващите решения за сигурност.

32. Решението да поддържа възможност за откриване на целенасочени атаки, посредством активно проучване и откриване на злонамерена инфраструктура и зловреден софтуер преди да бъдат активирани за използване от нападателите;

33. Решението да поддържа откриване и наблюдение на фишинг сайтове и хранилища на зловреден софтуер;

34. Възложителят при нужда да има възможност да заяви срещу допълнително заплащане предоставяне на поръчкови репорти свързани с различни заплахи, нападатели, риск и т.н..

35. Решението да включва достъп до анализатор от страна на производителя, който когато е необходимо да предоставя пояснения при специфични за клиента цели, проучвания и анализи;

36. Решението да предоставя разузнавателна информация за заплахите свързани с конкретни индустрии;

37. Решението да не събира никаква информация от вътрешната инфраструктура или прилежащи към нея компоненти;

38. Решението да може да предоставя WHOIS информация;

39. Решението да предоставя предупреждение в реално време при резултати от предварително дефинирани търсения;

40. Решението да предоставя различни възможности за визуализиране на резултатите от дадено търсене, като минимални аналитични изгледи да се включват:

- Timeline
- Table
- Map
- Source Map
- Feed.

41. Решението да оценява не само потенциалното въздействие на дадена уязвимост, но също и възможността за използване и дали в момента е активно използвана;

42. Решението да позволява на Възложителя да създава „Списъци за наблюдение“ на технологии и продукти, които попадат в активите на компанията. След това да се извършва проактивен мониторинг специално за тези активи, включително сигнали за всяко увеличаване на възможността за използване на дадена уязвимост или нейната критичност;

43. Решението да включва браузър разширение, чрез което да може да се четат индикатори от дадена уеб страница, като домейн, IP, URL, hash, CVE и да предоставя тяхната риск оценка в реално време. Това да може да се използва за разследване в реално време или за обогатяване на информацията от различните системи с уеб интерфейс в организацията;

44. Решението да се достави с включени минимум 25 броя годишно кредита/услуги за предприемане на действия от страна на производителя по премахване на съдържание като:

- Домейни/уеб сайтове с подобен URL адрес на марката, който хоства злонамерено или phishing съдържание.
- Злоупотреба с марката в социалните медии. Представяне на марката напр. Twitter профил използващ брандинг (лого) на организацията, туитващи връзки към измама с

криптовалута.

- Измамно съдържание или съдържание в нарушение на марката. Това може да се състои от фалшиви обяви за работа или фалшива връзка с клиент.
- Неоторизирани мобилни приложения. Мобилни приложения, използващи брандиране на организацията без разрешение; например дублиране на легитимно приложение или версия, която е била подправена (рекламен, злонамерен софтуер, шпионски софтуер и т.н., вградени в приложението, създавайки негативно изживяване за крайния потребител и причинявайки щети на марката).
- Сървъри за злонамерен софтуер, насочени към клиенти. Изпускане на зони, командни и контролни структури, пренасочвания на зловреден софтуер и изтегляния..

45. Решението да се достави с включена услуга за предоставяне на поръчкови репорти от производителя, свързани с различни заплахи, нападатели, рискове и т.н. – за минимум 6 репорта на година;

46. Предложеното решение да включва права за ползване на изискваните функционалности от минимум двама потребителя на Възложителя и интеграция с предложената от Изпълнителя SOAR система, за период не по-малък от 36 месеца.

2.3.3.5. Изискване към функцията - киберзащита на крайни точки

1. Да се доставят всички необходими лицензи с права за ползване на всички изисквани функционалности за защита на 3 500 (три хиляди и петстотин) работни станции в информационната система на Възложителя;

2. Решението да включва централизирана конзола за управление и наблюдение на всички защитени крайни точки;

3. Решението да включва функционалност за откриване/идентифициране на Fileless атаки и Zero-day атаки без да използва бази данни с репутация на IP адреси, DNS, URL, преки пътища/хешове или сигнатури;

4. Решението да използва статични и динамични алгоритми, базирани на изкуствен интелект за идентифициране на заплахи, включително Zero-day атаки;

5. Решението да включва един самостоятелен агент с функционалност за защита на крайни точки (EPP - Endpoint Protection Platform) и лов и отговор на заплахи на крайни точки (EDR - Endpoint Detection & Response);

6. Решението да включва функционалност за защита на крайни точки от тип десктоп с операционни системи Windows XP и следващи версии, macOS и Linux;

7. Решението да поддържа възможност за защита на сървъри с операционни системи Windows Server 2003 и следващи версии, и Linux, чрез закупуване на допълнителни лицензи за защита на сървъри;

8. Работата на агента да бъде напълно автономна и неговите функционалности да са независими от конзолата за управление, облака или ресурси външни за агента;

9. Агентът да може да открива и реагира на заплахи (Zero-day, Fileless, RAM-базирани, Zero-day експлойти, рансъмуер, криптокопачи, Lateral movement, APT) в реално време, независимо от състоянието (онлайн или офлайн) на мрежата на защитаваната крайна точка;

10. Решението да може да класифицира събитията/заплахите на защитаваните крайни точки, в минимум две категории: "Заплаха (Злонамерена заплаха)" и "Подозрителна дейност (Подозрителна заплаха);

11. Решението да включва минимум два режима на работа/политики за сигурност ("Предупреждение" или "Активна защита") за отговор на заплахи въз основа на извършената класификация на събитието/заплахата;

12. Решението да предоставя минимум следните възможности за автоматична реакция/действия при откриване на заплахи:

- Предупреждение - винаги да извежда съобщение за открита заплаха независимо от избрания режим на работа/политика за сигурност;
- Убиване на процес: Да спира и унищожава процеси в активно съдържание в документи, изпълними файлове и подчинени процеси, които се изпълняват извън нормалното поведение на крайната точка или не съответстват на нормалните действия на приложението, в което процесът се крие.
- Карантина: Да спира процесите, криптира изпълнимия файл и да го премества на ограничен път; Автоматично да дезактивира известни заплахи, преди да бъдат изпълнени.
- Прекъсване на връзката с мрежата на защитената крайна точка: (мрежова карантина или мрежова изолация) - Да спира комуникацията на крайната точка с други компоненти в мрежата освен между агента и конзолата за управление на решението. Всички функционалности на решението да са налични въпреки въведената мрежова изолация от агента;
- Възстановяване на конфигурационни промени: Да спира процеси, да поставя под карантина двоични файлове, да премахва свързани библиотеки, да изтрива изходни файлове и да възстановява конфигурацията на операционната система, приложенията и потребителските настройки до състоянието преди началото на атаката.
- Връщане назад: да възстановява състоянието на крайната точка до състоянието по време на създаването на моментната снимка на Volume Shadow Copy (VSS), връщайки промените, направени от злонамерения процес и свързаните с него ресурси. Агентът автономно и в реално време да може да възстанови данните от защитената точка в случай на атака от ransomware;.

13. Решението да поддържа следните модели на внедряване: SaaS (агент-> облачна SaaS услуга) или локално внедряване (виртуално устройство) или хибридно внедряване. Да бъде доставено в модел на локално (On-prem) внедряване, конзолата за управление на предложеното решение да бъде инсталирана в инфраструктурата на Възложителя;

14. Решението да поддържа следните механизми за откриване на злонамерен софтуер:

- Предварително изпълнение:

- сканиране и идентифициране на зловреден софтуер само при първоначална инсталация на решението за защита на крайни точки на базата на файлове, чрез репутация инициирано от конзолата за управление. Използването на този механизъм да не е задължително за да се гарантира, че всички функции за сигурност работят правилно и да не изисква актуализации на базата данни със сигнатури или актуализации на файлове със сигнатури за да работи;
- решението да може да идентифицира неизвестен базиран на файл злонамерен софтуер въз основа на статичен анализ използвайки алгоритми за машинно обучение автономно на крайната точка, без външни зависимости или външна обработка. Функционалността да не изисква използването на известни IoC (DNS, IP, URL, HASH) за да работи, откриването да работи в реално време, докато се осъществява достъп до операционна система или файл;

- По време на изпълнение:

- Агентът да може да идентифицира и реагира на атаки, използващи сложни хакерски техники (Fileless атаки, Zero-day уязвимости и злонамерен софтуер, злонамерени скриптове, странично движение, рансъмуер, троянски коне, APT и т.н.) Идентифицирането на тези заплахи да не изисква външни зависимости, човешка намеса или анализ на данни извън защитената крайна точка. Функционалността да работи в реално време, чрез използването на алгоритми с изкуствен интелект. Известен IoC (DNS,

IP, URL, HASH) не трябва да се изисква като средство за идентифициране на заплаха.

15. Решението да включва механизъм "Anti-Tamper" за защита срещу софтуерни манипулации от зловреден софтуер или крайния потребител. Този механизъм да бъде защитен с уникална парола за всяка крайна точка. Защитата от подправяне да бъде конфигурируема опция в политиката за сигурност с опции за Включено/Изключено състояние;

16. Решението да включва функционалност за създаване на политики за сигурност с активиране или деактивиране на отделни механизми за откриване на заплахи;

17. Решението да включва отворен API, който позволява интеграция с други решения, мониторинг на средата и автоматизация на процеси. Документацията на API да е достъпна в конзолата за управление;

18. Решението да включва Multi-Site или Multi-Tenancy архитектура, за напълно разделяне на създадения достъп в системата и осигуряване на административен достъп до конкретно местоположение, създадено според модела Multi-Site;

19. Решението да включва SSO - SAMLv2 удостоверяване;

20. Решението да поддържа двуфакторно удостоверяване (2FA) за административен достъп с Google Authenticator или Duo;

21. Решението да включва следните формати на syslog: CEF, CEF2, RFC-5424, STIX и IOC;

22. Решението да включва SSL и X.509 сертификати за криптиране и удостоверяване на транспорта на syslog;

23. Решението да включва функционалност за изпращане на текстови съобщения до потребителя на крайната точка, директно от конзолата за управление, дори когато агентът, работещ на крайната точка е в режим на мрежова изолация/мрежова карантина;

24. Агентът на решението да предоставя информация за групи към които е асоциирана крайната точка в Active Directory, включително Device и User AD атрибути. Конзолата за управление да не изисква свързване с Active Directory директно чрез ADFS или друг метод за получаване на необходимата информацията. Конзолата за управление на решението не трябва да е независим от състоянието на AD услугата;

25. Конзолата за управление да включва табло с информация, показващо списък с всички крайни точки с възможност за филтриране въз основа на атрибути като ОС, тип крайна точка, версия на агент, налични уязвимости, AD атрибути, телеметрична информация, IP адресиране, хардуерни характеристики, брой CPU, Mac адреси , интерфейси, име на хост, име на група, домейн). Списъкът трябва да бъде достъпен за преглед на крайни точки за инвентаризация, прилагане на действия към подмножество от крайни точки или картографиране на крайни точки към групи. Да предоставя възможност за преглед на подробности за крайната точка като аспекти на телеметрията, състояние на крайната точка, приложения и да предоставя следните възможности за действия: Прекъсване на връзката/Свързване с мрежата (мрежова карантина, Рестартиране на ОС, Изключване на системата, Изпращане на съобщение до потребителя, Деинсталиране на агент, Преглед заплахи;

26. Решението да взима контрол над локалната защитна стена на защитената крайната точка. Правилата на защитната стена да могат да работят със следните параметри: FQDN, IP, CIDR. Функционалността да се поддържа за операционни системи: Windows, Linux и macOS;

27. Решението да включва функционалност за контрол на устройства с USB и Bluetooth интерфейс, които опитват да получат достъп до защитената крайна точка. Да се поддържа създаване на отделни политики на база група от крайни точки;

28. Решението да включва функционалност за управление на уязвимостите на приложенията, инсталирани на защитените крайни точки, и да предоставя CVE информация, свързана с откритата уязвимост;

29. Решението да има възможност за бъдещо надграждане с допълнителен

лиценз/лицензи предоставящи следните функционалности:

- Модул, който да се интегрира в конзолата за управление за автоматично откриване на IoT устройства в мрежата, без нужда от сензори, снифери или друг подобен хардуер, използващ методи за откриване. чрез Agent, DHCP, DNS, SSDP, PING, Neighbor, SCAN, позволяващ отдалечено инсталиране на агентски софтуер на открити станции без такъв софтуер да е наличен за операционни системи Windows, Linux, macOS.
- Търсене на IoT устройства въз основа на клас устройства (видео, мобилно устройство, принтер, инфраструктура, сървър, работна станция, IP телефон, съхранение, виртуална машина)
- IoT табло за управление с визуализация на процента на управляваните, неуправляваните и неподдържаните устройства и подробна информация за устройствата, включваща име на хост, IP адрес, версия на ОС, MAC адрес, използвани методи за откриване, отворени TCP и UDP портове.

30. Решението да има възможност за бъдещо надграждане с допълнителен лиценз/лицензи предоставящи следните функционалности използващи същия агент и конзола за управление:

- Автоматично и автономно извършване на индексиране, корелация и генериране на идентификатор на свързани събития в защитената среда;
- Генериране на справки тип "дърво на процесите", съдържащи информация за анализ на всички под-събития (IP, DNS, ФАЙЛОВЕ, РЕГИСТРИ, ПРОЦЕСИ, URL адреси и т.н.), които съставляват дадено събитие;
- Създаване на персонализирани правила за откриване на заплахи, които задействат предупреждения и автоматични действия, когато правилата открият търсения тип поведение на крайна точка;
- Remote Shell за изпълняване на команди на крайната точка от администратора;
- Добавяне на персонализирани Powershell (Windows) и Bash (Linux, Mac) скриптове към централно хранилище;
- Съхранение на данни за лов и отговор на заплахи на крайни точки (EDR) за период до 365 дни.

31. Конзолата за управление на предложеното решение трябва да бъде инсталирана в инфраструктурата на Възложителя, като минималните изисквания за необходимите ресурси не трябва да надвишават: 4 CPU, 8G RAM, 100GB SSD дисково пространство.

2.3.3.6. Изискване към функцията - осигуряване на отдалечен достъп през криптиран канал за комуникация с включени функционалности за инспекция, защита на крайни устройства и VPN без агент (Clientless VPN)

1. Предложеното решение да бъде съвместимо с два броя защитни стени, модел PA-5220, които са внедрени в сървърната и мрежовата инфраструктура на АЕЦ „Козлодуй“.

2. Да бъде осигурено дублиране на системата, с цел осигуряване на резервираност и непрекъсваемост на услугите;

3. Решението да предоставя функционалности за инспекция и защита на крайни устройства преди изграждането на VPN, която да включва минимум следните методи:

- Patch management
- Host anti-spyware
- Host anti-malware
- Host firewall

- Disk encryption
- Disk backup
- Data loss prevention
- Customized HIP conditions

4. Решението да предоставя възможност за изграждане на отдалечен достъп (VPN) от мобилни устройства включващи минимум следните операционни системи:

- Microsoft Windows and Windows UWP
- Apple macOS
- Apple iOS and iPadOS
- Google Chrome OS
- Android OS
- Linux OS (Red Hat, CentOS, Ubuntu, Raspbian)
- IoT devices

5. Решението да предлага минимум следните методи за защита на клиентския трафик:

- IPsec
- чSSL
- Clientless VPN
- Per-app VPN on Android, iOS

6. Решението да поддържа IPv4 и IPv6 мрежови протоколи;

7. Решението да може да се стартира автоматично заедно с клиентска операционна система;

8. Решението да предоставя минимум 15 000 SSL VPN конкурентни потребителя и минимум 2500 Clientless VPN тунела за период от минимум 36 месеца;

9. Да бъде посочи партиден номер на производителя за поддръжката.

Софтуер - инсталиране и конфигуриране.

Изпълнителят да предостави на Възложителя пълен инсталационен пакет на софтуера на всички модули на системата за защита от кибератаки.

2.3.4. Част ПБ (Пожарна безопасност)

Част "Пожарна безопасност" да се разработи с обхват и съдържание съгласно Приложение № 3 от Наредба № 1з-1971 от 29.10.2009 г. за строително-технически правила и норми за осигуряване на безопасност при пожар.

За част "Пожарна безопасност" Изпълнителят да разполага с минимум един проектант с пълна проектантска правоспособност (ППП) по интердисциплинарна част "Пожарна безопасност - техническа записка и графични материали".

Проектните решения, които засягат оборудване в състава или в помещенията на системите за безопасност и системите, важни за безопасността трябва да са съобразени с изискванията за осигуряване на пожарна безопасност, определени в Наредба за осигуряване безопасността на ядрените централи от 2016.

2.3.5. Част ПБЗ (План за безопасност и здраве)

2.3.5.1. Част ПБЗ да се изготви съгласно Наредба № 2 от 22.03.2004г. за минималните изисквания за здравословни и безопасни условия на труд при извършване на строителни и монтажни работи. Обяснителната записка да е разработена за дейностите в настоящия проект;

Схеми и чертежи съгласно чл. 10 на Наредба № 2 от 22.03.2004 г. за минималните

изисквания за здравословни и безопасни условия на труд при извършване на строителни и монтажни работи.

2.3.5.2. Конструкцията на автономните изделия трябва да изключва възможността за достъп на обслужващия персонал по време на работа, при провеждане на техническото обслужване и ремонт до частите, намиращи се под опасно напрежение, а така също до неизолираните части, работещи при ниско напрежение и неподсъединени към защитното заземяване.

2.3.5.3. Изисквания, необходими за изготвяне на проекта за организация на монтажа:

- Описание на факторите на работната среда, които трябва да се отчетат при проектирането, за работа на персонала с ново проектираното оборудване, както и изисквания за класа на помещенията по пожароопасност и взривоопасност.
- график и условия за монтаж - ПГР и ориентировъчни срокове;
- условия за използване на кранове, складове и др.;
- условия за монтаж, изпитания и въвеждане в експлоатация.

За всяка от посочените в това ТЗ части на Работния проект Изпълнителят трябва да представи:

Обяснителна записка (Описание на проектното решение) - Изпълнителят да опише приетите проектни решения и функции на отделните части от системата за защита от кибератаки, разположение на оборудването, хардуерни елементи, софтуер и допълнителни приложения, мрежови връзки, архитектура и т.н.

Записките се изготвят в обем не по-малък от определените в Глави от 8 до 17 на НАРЕДБА №4 от 21.05.2001 за обхвата и съдържанието на инвестиционните проекти.

Взаимовръзки със съществуващия проект - Изпълнителят да опише обхвата на проектираната система за защита от кибератаки, отделните общи точки на свързаност с информационната система на АЕЦ „Козлодуй“. При наличие на допълнителни изисквания към взаимовръзките със съществуващия проект те се описват конкретно.

Изисквания към работата на оборудването - да се опишат всички изисквания, отнасящи се към работата на отделни елементи на оборудването, по отношение на бъдещата му експлоатация и поддръжка. Системата да има експлоатационен живот не по-малък от 10 години след въвеждане в експлоатация.

Изчислителна записка и пресмятания - представят се изчисленията, обосноваващи проектните решения по отношение функционалност, изискания към хардуерният ресурс, оразмеряване на конструктивните елементи и др.

Чертежи, схеми и графични материали - да се разработят необходимите графични изображения (чертежи) на приетите проектни решения, по които могат да се изпълняват монтажни работи, планове на разположение на оборудването и логическа схема системата включваща проектните решения за киберзащита и взаимовръзката им със съществуващата информационна система.

Спецификации - проекта да включва спецификация на предлаганите софтуерни решения, оборудването и материалите, които ще бъдат доставени по време на изпълнение на проекта, както и необходимите лицензи, спецификация на резервни части и/или консумативи.

Техническа спецификация - Да се представи техническа спецификация, в която да е описано основното оборудване, необходимо за доставка.

Списък на норми и стандарти

- НП-001-15, „Общие положения обеспечения безопасности атомнмх станций";
- НП-031-01, "Норми проектирования сейсмостойких атомнмх станции" 2001;

3. Изисквания към доставката на оборудване и материали

Доставката да бъде изпълнена в обем и с качество, в съответствие с предвиденото в работния проект и техническите спецификации към отделните части.

3.1. Класификация на оборудването

Съгласно НП-001-15 „Общие положения обеспечения безопасности атомнмх станций", обекта на техническото задание се отнася към елементи за нормална експлоатация 3 клас (3-Н).

3.2. Категория по сеизмоустойчивост

В съответствие с т.3.2 от НП-031-01, оборудване сеизмична категория 3 се квалифицира в съответствие с действащите нормативни документи, изискванията на които се разпространяват на граждански и промишлени обекти. В България това е системата Еврокод за стоманобетонни и стоманени конструкции. Националният сеизмичен код да бъде приложен, като се използват сеизмичните характеристики за ниво ПЗ (максимално ускорение, етажни спектри на реагиране) за мястото на монтиране в АЕЦ "Козлодуй".

3.3. Квалификация на оборудването

3.3.1. Климатични условия

- Новата система не трябва да изисква преработка на съществуващите системи за поддържане на климата в помещения;
- Новата система не трябва да изисква техническо обслужване повече от веднъж годишно.

Температура

- Новото оборудване трябва да бъде способно да работи непрекъснато в интервал +10°C до +35°C температура на околния въздух - нормални експлоатационни предели в съществуващите помещения за оборудването;
- Новото оборудване трябва да може да се съхранява в помещения с температура на въздуха +5°C до +50°C;
- Проектът трябва да предвиди необходимото охлаждане на новите шкафове, с цел температурата във вътрешността на шкафовете да не нараства с повече от 10°C, спрямо околната температура, следствие на работата на системата.

Влажност

- Оборудването трябва да остава работоспособно при относителна влажност на въздуха - до 80% при +25°C с неограничена продължителност на въздействието.

3.3.2. Електрозахранване

- Оборудването трябва да работи в допустимите граници с два независими източника на електрическо захранване;
- Оборудването трябва да съхрани работоспособност по време на загубата на едното захранване и след това:
- Оборудването трябва да работи в допустимите граници с АС захранване с напрежение между 187 и 242V и честота между 47 и 53Hz и съдържание на хармоници по-малко от 6%.

Номиналното напрежение трябва да бъде 220V при номинална честота от 50Hz;

- Ремонтът или замяната на резервирано захранване по време на работа не трябва да влияе на експлоатацията на системата;

3.4. Физически и геометрични характеристики

Доставеното оборудване да бъде съобразено с изискванията за монтаж в 19“ комуникационен шкаф.

3.5. Характеристики на материалите

Няма отношение.

3.6. Химични, механични, металургични и/или други свойства

Няма отношение.

3.7. Условия при работа в среда с йонизиращи лъчения

Помещение 5AE128/1, в което ще бъде разположено оборудването, обект на техническото задание, не подлежи на категоризация по радиационна безопасност.

3.8. Изисквания към срок на годност и жизнен цикъл

3.8.1. Жизненият цикъл на системата, към момента на монтирането и трябва да бъде във фаза при производителя “Търговска наличност” (произвежда се, поддържа се, на пазара са налични всички необходими резервни част и модули).

3.8.2. Проектният живот на новата система трябва да бъде не по-малко от 10 години. Осигуряването на поддръжка на система от Изпълнителя трябва да бъде осигурено за срок най-малко до 3 (три) години след въвеждането и в експлоатация.

3.8.3. За хардуерните и софтуерните компоненти на системата (сървъри, софтуерни пакети, операционна система), чийто проектен живот е по-кратък от 10 години, се изисква да бъде осигурена възможността за ъпдейт, ъпгрейд и мигриране, така, че да бъде постигнат изисквания проектен живот от минимум 10 години за системата като цяло.

3.9. Допълнителни характеристики

Всички проектни решения предварително да се съгласуват с Възложителя.

3.10. Изисквания към доставката и опаковката

Всички хардуерни компоненти да бъдат доставени в АЕЦ “Козлодуй” с опаковка, изключваща повреждането им от атмосферни условия по време на транспорт и при извършване на товаро-разтоварни операции.

Доставката да включва специализирани софтуерни инструменти и устройства за проверка, ремонт, поддръжка и техническо обслужване.

3.11. Товаро-разтоварни дейности

Товаро-разтоварните дейности за транспортиране на оборудването до мястото на монтаж са задължение на Изпълнителя.

3.12. Транспортиране

3.12.1. Оборудването е необходимо да е опаковано и етикетирано в съответствие с изискванията на производителя. Обемното оборудване трябва да е пакетирано и подредено върху стандартни европалета по начин, позволяващ преброяването и механизираното му разтоварване.

3.12.2. Транспортирането на оборудването до мястото за монтаж е задължение на Изпълнителя на монтажните дейности.

3.13. Условия за съхранение

Съхранението на оборудването да се извърши в съответствие с изискванията на производителя.

4. Изисквания към производството

4.1. Правилници, стандарти, нормативни документи за производство и изпитване

Няма отношение.

4.2. Тестване на продуктите и материалите по време на производство

Няма отношение.

4.3. Контрол от страна на „АЕЦ Козлодуй" ЕАД по време на производството

Няма отношение.

4.4. Мерки за безопасност против замърсяване с радиоактивни вещества и опасни продукти

Няма отношение.

4.5. Отговорности по време на пуск

4.5.1. Изпълнителят ръководи дейностите по реализацията на проекта.

4.5.2. Изпълнителят е длъжен да осигури авторски надзор и предаване на актуализирани проектни схеми и чертежи, отразяващи направените изменения в проекта по време на монтажа и функционални изпитания.

4.6. Състояния на повърхностите и полагане на покрития

Няма отношение.

4.7. Условия за безопасност

В пълен обем да се отчетат изискванията за осигуряване на безопасността, определени в част ПБЗ (по т.2.3.6.) на работния проект и мерките за пожарна безопасност съгласно част "Пожарна безопасност" (по т.2.3.5).

Оборудването и материалите, съдържащи опасни компоненти трябва да бъдат маркирани/етикетирани съгласно нормативната уредба по околна среда.

5. Изисквания към строителните дейности

Дейностите ще се извършват в:

Защитена зона - зона на площадката на АЕЦ "Козлодуй" с организирана пропускателна система, която включва: гл. портал 5.

Зона с контролиран достъп - зона около площадката на АЕЦ "Козлодуй" с контролиран достъп на КПП Запад, КПП Обзорно място, Административни сгради.

5.1. Контрол на строително-монтажните работи

5.1.1. Инвеститорски функции по отношение на изпълнение, приемане, контрол, координация и отчет на работата се изпълняват от управление "Инвестиции", отдел ИК.

5.1.2. Планираният технически и независим контрол на изпълнението на дейностите ще се изпълнява от определените от Възложителя длъжностни лица от Управление ИиКТ, Отдел ИСиКТ.

5.2. План за изпълнение на строителните работи

Да се изготви график за изпълнение на дейностите, който трябва да включва отделните етапи, дейности, сроковете за изпълнението им и необходимите ресурси. В графика трябва да се включат и дейностите, изпълнявани от АЕЦ „Козлодуй", които влияят върху изпълнението на дейността от Изпълнителя. За по-сложните и продължителни дейности се указва и критичния път.

Графикът задължително се съгласува с АЕЦ „Козлодуй". При необходимост графикът се актуализира по време на изпълнение на строителните дейности.

5.3. Условия и дейности, които трябва да се изпълнят от „АЕЦ Козлодуй" ЕАД

5.3.1. Допускане на персонала на изпълнителя до площадката на АЕЦ „Козлодуй", съгласно изискванията на "Инструкция по качество. Работа на външни организации при сключен договор", ДБК.КД.ИН.028 и по реда на „Инструкция за пропускателен режим в АЕЦ "Козлодуй"", 10.ФЗ.00.ИН.015;

5.3.2. Разрешение за изпълнение на работата (монтажни, пусково-наладъчни дейности) на персонала на Изпълнителя, на базата на съгласувания от Възложителя подробен график;

5.4. Условия и дейности, които трябва да се изпълнят от Изпълнителя

5.4.1. При изпълнение на дейностите, свързани с монтажа, да се спазват изискванията на Монтажната документация и монтажни процедури, включващи описание на дейностите по монтаж на устройствата, присъединяване и закрепване на кабелите за връзка с външни устройства, проверка работоспособността и тестване на устройствата.

5.4.2. По никакъв начин да не се допуска загуба на информация, затруднения с трафика на данни, отказ на мрежово оборудване, откази на услуги предоставяни в информационната система (същите ще бъдат в работоспособност по време на въвеждане на системата за защита от кибератаки в експлоатация).

5.4.3. Монтажните работи да се извършват със заявка и наряд при спазване на изискванията на ДБК.КД.ИН.028 " Инструкция по качество. Работа на външни организации при сключен договор" и стриктно спазване на изискванията по безопасност и охрана на труда и поддържане на експлоатационния ред.

5.4.4. Изпитания на софтуера

Изпълнителят, съвместно с Възложителя, извършва тестване и функционални изпитания на Програмното осигуряване при въвеждане в експлоатация на софтуера, съгласно работни програми и методики за изпитания, разработени от Изпълнителя.

5.4.5. Валидация на софтуера.

Функционалните изпитания на софтуера на системата за защита от кибератаки да докажат, че софтуерът изпълнява в пълен обем заложените функции във всички проектни режими на експлоатация.

5.5. Монтаж и въвеждане в експлоатация

5.5.1. Изпълнителя работи по одобрен работен проект.

5.5.2. Монтажните работи, да се извършат с заявка и наряд при спазване на изискванията на ДБК.КД.ИН.028„Инструкция по качество. Работа на външни организации при сключен договор“ и стриктно спазване на изискванията по безопасност и охрана на труда и поддържане на експлоатационния ред.

5.5.3. Приемането и изпълнението на СМР става съгласно, Наредба №3 от 31.07.2003 г. за съставяне на актове и протоколи по време на строителството, Правила за извършване и приемане на строителни и монтажни работи, Наредба №РД-02-20-1 от 12.06.2018 г. за технически правила и нормативи за контрол и приемане на електромонтажни работи и Плана за контрол на качеството (ПКК).

5.5.4. След приключване на монтажа е необходимо Възложителят да инспектира извършената работа, а Изпълнителя да предаде акт за извършена работа и акт за завършен монтаж.

6. Изисквания към други дейности, необходими за изпълнение на поръчката

Няма отношение.

7 . Нормативно-технически документи, приложими към строително-монтажните работи и въвеждане в експлоатация

“Правилник за безопасност и здраве при работа в електрическите уредби на електрически и топлофикационни централи и по електрически мрежи”, София, 2004г.
“Наредба №2 от 22.03.2004 г. за минималните изисквания за здравословни и безопасни условия на труд при извършване на строителни и монтажни работи”, София,
“Наредба №3 от 9.06.2004 г. за устройството на електрическите уредби и електропроводните линии”,
“Наредба №9 от 9.06.2004 г. за техническата експлоатация на електрически централи и мрежи”
“Наредба №16-116 от 8.02.2008 г. за техническата експлоатация на енергообзавеждането”,
“Наредба №3 от 31.07.2003 г. за съставяне на актове и протоколи по време на строителството”
„Наредба № РД-02-20-1 от 12.06.2018 г. за технически правила и нормативи за контрол и приемане на електромонтажни работи”;
“Наредба № Із-1971 от 29.10.2009 г. за строително-технически правила и норми за осигуряване на безопасност при пожар”.
“Наредба № 8121з-647 за правилата и нормите за пожарна безопасност при експлоатация на обектите”.

8 . Документи, които се изискват при доставка, монтаж и въвеждане в експлоатация

8.1.Документи, изискващи се на етап доставка:

- Заводска документация: Инструкции за експлоатация, ремонт и техническо обслужване на оборудването;
- Сертификати/ Декларации за съответствие на доставеното оборудване и материали, с които се потвърждава, че доставяното оборудване/резервни части отговаря на

изискванията, указани в заводската документация с посочване на несъответствията, ако има такива;

- Лицензи: Всички лицензи трябва да са на името на "АЕЦ Козлодуй" ЕАД и ли при изписване на латиница Kozloduy NPP Plc
- Протоколи от проведен входящ контрол.

8.2. Документи, изискващи се на етап монтаж и въвеждане в експлоатация:

- Съгласуван график за изпълнение на монтажните работи;
- Планове за контрол на качеството на отделните дейности;
- Инструкция по експлоатация;
- Програма за обучение на поддържащ и инженерен персонал;
- Изпълнителят е длъжен да използва "Заповедна книга на строежа" при извършване на инвестиционните дейности, съгласно чл.7, ал.3, т.4 от НАРЕДБА № 3 от 31.07.2003 г. за съставяне на актове и протоколи по време на строителството, в която да въвежда измененията в проекта по време на строително-монтажни работи. В случай на проектно изменение се издава заповед, която се записва в Заповедната книга. След приключване на работата заповедната книга се предава за архивиране заедно с останалите отчетни документи;
- По време на монтажните дейности е възможно да възникнат изменения в първоначалния проект. Измененията се документират, съгласно чл.8, ал.2 от НАРЕДБА № 3 от 31.07.2003 г. за съставяне на актове и протоколи по време на строителството. Чертежите се наричат "екзекутив", маркират се с червено мастило на местата, претърпели изменение и след приключване на работата се предават на АЕЦ "Козлодуй".

9. Входни данни

9.1. Изпълнителят да подготви и предостави списък на необходимите му входни данни за изпълнение на дейностите по настоящето техническо задание след сключване на договор по реда на "Инструкция по качеството. Предаване на входни данни на външни организации", № ДОД.ОК.ИК.1194/*".

9.2. Входните данни, необходими за изпълнение на дейностите по настоящето техническо задание, ще бъдат предавани на Изпълнителя във вида и формата, в която са налични в АЕЦ "Козлодуй".

9.3. Входните данни се предават на Изпълнителя след сключване на договор.

9.4. Необходимите входни данни, които документално не са налични да се снемат от Изпълнителя, със съдействието на Възложителя, чрез обходи и заснемане на съществуващото положение по място, при спазване на изискванията за осигуряване на достъп до площадката на АЕЦ "Козлодуй", съгласно ДБК.КД.ИН.028.

9.5. При липса на входни данни, Изпълнителят да ги разработи за своя сметка, със съдействието на Възложителя.

9.6. Ако е необходимо да се предоставят други входни данни, те се изготвят допълнително като отделен документ по реда на "Инструкция по качеството. Предаване на входни данни на външни организации", № ДОД.ОК.ИК.1194/*.

10. Входящ контрол

10.1. Всички компоненти на оборудването да бъдат доставени на площадката на АЕЦ

"Козлодуй".

10.2. Доставеното оборудване да премине общ входящ контрол по реда на "Инструкция по качество за провеждане на входящ контрол на доставените материали, суровини и комплектуващи изделия в АЕЦ "Козлодуй", №10.УД.00.ИК112/*.

10.3. Входящият контрол за софтуерните продукти и лицензи се извършва чрез проверка в профила на Възложителя в портала на съответният доставчик за активиране на съответното количество лицензи, и се документира с двустранен приемо-предавателен протокол.

11. Изходни документи, резултат от договора

11.1. На етап проектиране:

- Работен проект в обем и съдържание, съгласно т.2 от настоящето ТЗ.
- План за качество за процеса на проектиране (с положени подписи на изпълнени операции);
- Подробен график за проектиране, монтаж и конфигуриране;
- Техническа спецификация на новото оборудване и софтуер;
- Проектно описание на софтуера;

11.2. На етап доставка:

Документи съгласно т.8.1 от настоящето ТЗ и:

- Декларации за съответствие и декларации за произход на материалите, вложени от Изпълнителят при извършване на дейностите по отделните части на проекта, изискващи се от съответните наредби за съществените изисквания в РБ, представени на български език;
- Програма за обучение;
- Програма и методика за тестване, верификация и валидация на софтуера (програма за функционални изпитания);

11.3. На етап монтаж:

Документи съгласно т.8.2 и :

11.3.1. Отчетни документи, които се изготвят от Изпълнителя по време на работата по договора и са в съответствие с изискванията на Наредба № 3/31.07.2003 г. за съставяне на актове и протоколи по време на строителството.

11.3.2. По време на изпълнение и след завършване на монтажните работи, инсталирането и конфигурирането на софтуера, Изпълнителят да представи следните документи:

- Акт за завършен монтаж;
- Актове за извършена работа;
- Други документи, при необходимост, в зависимост от изпълнените монтажни дейности.

11.4. След монтаж и въвеждане в експлоатация:

- Протоколи за монтаж и изпитване, актове и протоколи по време на строителството, съгласно НАРЕДБА №3 за съставяне на актове и протоколи по време на строителството, и/ или отчетни документи, изисквани съгласно действащите инструкции в АЕЦ

"Козлодуй";

- Изпълнителят трябва да предаде актуализирани проектни схеми и чертежи, преиздадени с пореден номер на редакция, отразяващи направените изменения в проекта по време на монтажа, в електронна форма и на хартиен носител, подпечатани на всяка страница с червен печат "Екзекутив" в срок не по-късно от 2 месеца след приключване на ПНР. Актуализираните проектни схеми се предават в 3 екземпляра на хартиен носител и 1 екземпляр на магнитен носител, в оригинален формат на изготвяне;
- Протоколи от тестване, верификация и валидация на софтуера (функционални изпитания);
- Инструкции за експлоатация;
- Инструкция за инсталиране на системата;
- Ръководство за системния администратор за администриране на системата за защита от кибератаки;
- Ръководство за потребителя на системата за защита от кибератаки;
- Протоколи за завършено обучение на персонала на АЕЦ "Козлодуй" за софтуерна поддръжка на системата;
- Документите изготвени на етап монтаж влизат в сила след утвърждаването им от упълномощените лица от АЕЦ "Козлодуй".

12. Критерии за приемане на работата

12.1. Дейностите по проектиране се считат за приключени, след преглед и приемане от страна на АЕЦ "Козлодуй" на работния проект без забележки. Този етап се приема на специализиран технически съвет (СТС), за което се оформя Протокол. Към следващия етап се преминава след утвърждаване на Протокола за приемане на Работния проект без забележки.

12.2. Дейностите по доставка се считат за приключени, след успешно проведен общ входящ контрол, по установен ред в АЕЦ "Козлодуй" , съгласно "Инструкция по качество за провеждане на входящ контрол на доставените материали, суровини и комплектуващи изделия в АЕЦ "Козлодуй", №10.УД.00.ИК.112/* и подписан протокол за входящ контрол без забележки.

12.3. Приемането и изпълнението на монтажа, инсталирането и конфигурирането на софтуера става съгласно Правила за изпълнение и приемане на строително-монтажните работи /ПИПСМР/, Наредба № РД-02-20-1 от 12.06.2018 г.и конкретния План за контрол на качеството.

12.4. Изпълнение в пълен обем и съответното качество на предвидените дейности в различните части на проекта и представен протокол за проведено обучение.

12.5. Предадена отчетна документация, съгласно "Наредба № 3 от 31.07.2003 г. за съставяне на актове и протоколи по време на строителството".

12.6. Успешно проведени настройки, положителен резултат от проведените функционални изпитания, 72-часови проби софтуерните продукти и оборудването, по изготвени от Изпълнителя и утвърдени от Възложителя програми.

13. Изисквания за осигуряване на качеството

13.1. Система за управление (СУ) на Изпълнителя

13.1.1. Изпълнителят да прилага сертифицирана Система за управление на качеството в съответствие с БДС ISO 9001:2015 „Системи за управление на качеството. Изисквания" или еквивалентно/и за дейности в обхвата на ТЗ.

13.1.2. Изпълнителят да прилага система за управление на сигурността на информацията по стандарт ISO/IEC 27001 или еквивалентно/и, за дейностите в обхвата на ТЗ.

13.1.3. Изпълнителят уведомява АЕЦ "Козлодуй" за настъпили структурни промени или промени в документацията на СУ на Изпълнителя, свързани с изпълняваните дейности по договора.

13.2. Програма за осигуряване на качеството (ПОК)

13.2.1. Изпълнителят да изготви Програма за осигуряване на качеството (ПОК), описваща прилаганата система за управление при изпълнение на дейностите в обхвата на ТЗ. Програмата служи за определяне на подробен график, отговорностите по всяка от задачите по договора и ред за изпълнението им. Представя се в дирекция БиК до 20 календарни дни след подписване на договора.

13.2.2. Програмата е предпоставка за стартиране на дейностите по договора, подлежи на преглед и съгласуване от страна на „АЕЦ Козлодуй" ЕАД и трябва да е изготвена на основание на:

- настоящето техническото задание и договора;
- системата за управление на Изпълнителя;
- примерно съдържание, предоставено от Възложителя;
- други стандарти и нормативни документи, имащи отношение към осигуряване на качеството в зависимост от вида на работата.

13.3. План за контрол на качеството (ПКК)/ План за контрол и изпитване (ПКИ)

13.3.1. Изпълнителят да изготви планове за контрол на качеството (ПКК) за дейностите по различните етапи (проектиране, доставка и монтаж). В ПКК да бъдат конкретно определени технологичната последователност на операциите по отделните дейности, регламентиращите документи за изпълнението им, точките на контрол от страна на Изпълнителя и на Възложителя и генерираните отчети и записи.

13.3.2. ПКК трябва да включват всички дейности, които са ключови по отношение на качественото изпълнение на обхванатия етап.

13.3.3. Не по-късно от 1 (един) месец преди началото на монтажните работи, Изпълнителят да изготви детайлни ПКК за изпълнението на монтажните работи по ТЗ с указани точки на контрол от страна на Изпълнителя и на Възложителя за всяка от дейностите, включени в плана. За дейностите по различните обекти да се изготвят отделни ПКК.

13.3.4. ПКК подлежат на проверка и съгласуване от отговорните лица на Възложителя.

13.3.5. При достигане на точка за контрол изпълнението на дейностите се задържа до извършване и документиране на планирания контрол. Работата по договора продължава след положителен резултат от контрола.

13.4. Одит от страна на „АЕЦ Козлодуй" ЕАД (одит от втора страна)

13.4.1. АЕЦ "Козлодуй" има право да провежда одити на системата по качество на Изпълнителите при спазване изискванията на 10.ОиП.00.ИК.049 "Инструкция по качество. Организация и провеждане на одит на външни организации /одит от втора страна/".

13.4.2. АЕЦ "Козлодуй" има право да извършва инспекции и проверки на дейностите,

извършвани на площадката.

13.5. Управление на несъответствията

13.5.1. Изпълнителят да изготви и поддържа в актуално състояние списък на несъответствията, възникващи по време на доставката, монтажа и изпитания. Изпълнителят е длъжен да уведомява и съгласува с Възложителя за предприетите коригиращи мерки.

13.5.2. Изпълнителя докладва на АЕЦ "Козлодуй" за:

- несъответствията, открити в хода на изпълнение на дейностите по договора;
- взетите решения за разпореждане с несъответстващия продукт/услуга.

13.6. Професионална компетентност (квалификация) на персонала на Изпълнителя

13.6.1. Изпълнителят да разполага с минимум по един проектант с валидно удостоверение за пълна проектантска правоспособност (ППП) от камарата на инженерите в инвестиционното проектиране за изпълнение на всяка част от проекта. Допустимо е един проектант да изпълни повече от една част на проекта.

13.6.2. Проектантът, който ще изпълнява проектирането по част "Пожарна безопасност" да притежава удостоверение за пълна проектантска правоспособност по част Пожарна безопасност с маркиран раздел "Пожарна безопасност-техническа записка и графични материали".

13.6.3. За изпълнение на работите на площадката на АЕЦ "Козлодуй", изпълнителят трябва да осигури минимум 2 (двама) специалиста, притежаващи сертификат за инженер по мрежова сигурност, издаден от производителя на предлаганото оборудване и софтуер или от упълномощен от него представител за целите на интегриране на доставените системи. Доказва се с прилагане на копие на сертификата.

13.6.4. Персоналът, който ще изпълнява работи на площадката на АЕЦ "Козлодуй", отнасящи се до монтажа на системите трябва да наброява като минимум 2 (двама) човека, притежаващи не по-ниска от 3 (трета) и 1(един) с не по-ниска от 4 (четвърта) квалификационна група съгласно "Правилник за безопасност при работа в електрически уредби на електрически и топлофикационни централи и по електрически мрежи" (ПБЗР-ЕУ).

13.6.5. Изпълнителят трябва да представи списък на персонала, който ще изпълнява дейностите, с информация за притежавано образование, опит, квалификация и заемана длъжност/роля в проекта със съответните документи доказващи опита и познанията в проектиране, изграждане и внедряване на системи в областта на киберсигурността и/или мрежовата и информационна сигурност.

13.7. Специфични изисквания по осигуряване на качеството

13.7.1. Изпълнителят е длъжен да спазва националното законодателство.

13.7.2. Навсякъде в настоящото техническо задание, където се изисква спазване на конкретно посочен стандарт може да бъде приложен еквиваленен.

13.7.3. Специфични изисквания по отношение на осигуряване на качеството:

- обозначаването на оборудването в проекта трябва да се извършва по правилата за присвояване на технологични обозначения в АЕЦ „Козлодуй";
- корекции в проектната документация се въвеждат по решение на СТС чрез издаване на нова редакция или внасяне на изменения (забележки от писмените становища) със запазване на действащата редакция. Контрол по внасяне на измененията се извършва от

членовете на СТС, определени в заповедта. Контролът по внасяне на измененията се документира;

- проектът се предава в три (3) екземпляра на български език и един (1) екземпляр на оригиналния език, при условие, че е различен от български. Проектната разработка да бъде заверена с печат за пълна проектантска правоспособност, за съответната част;
- проектът се предава и на електронен носител (CD), съдържащо: файлове в оригиналния формат на изготвяне на документите и pdf файлове, създадени чрез използване на сканираща техника с подписи и печати на проектантите;
- проектът да съдържа списък на всички използвани от проектанта проектни основи, ясно обозначени с наименование на документа, точката от документа, която поставя конкретните изисквания, и изискванията, поставени в ТЗ. Данните от предоставените от АЕЦ "Козлодуй" документи, съдържащи входни данни също се включват в този списък;
- проектът да съдържа списък на всички документи, които са изготвени в резултат на проектирането с наименование, индекс, дата на утвърждаване и последна редакция към момента на предаването му - на съответния етап или окончателно;
- когато по време на изпълнение на монтажните работи възникват несъществени изменения от одобрения проект, тези изменения се документират съгласно чл.8, ал 2 от Наредба 3 от 31.07.2013 г. за съставяне на актове и протоколи по време на строителство. Чертежите се наричат „екзекутив", маркират се с червено мастило на местата, претърпели изменение и след приключване на работа са предават на АЕЦ "Козлодуй";
- изготвеният проект се приема от страна на АЕЦ "Козлодуй" на специализиран технически съвет (СТС). Приемането на проекта на СТС не освобождава проектанта от отговорност, а служи само за определяне на целесъобразност и приемливост на представените проектни решения;
- екзекутивите (работен екзекутив) се изготвят от Изпълнителя и се предават със строителните книжа на Възложителя в 3 екземпляра на хартиен носител и на 1 оптичен носител, записани в pdf формат;
- Проектните части да бъдат заверени с печат за пълна проектантска правоспособност и „подпис", за съответната част.

13.7.4. Използваните в проекта суровини, материали и комплектуващи изделия трябва да отговарят на изискванията по отношение на забраната и ограниченията за употреба на определени опасни вещества, препарати и изделия, въведени с Приложение XVII на Регламент (ЕО) №1907/2006 от 18 декември 2006 година относно регистрацията, оценката, разрешаването, и ограничаването на химикали (REACH).

13.8. Обучение на персонал на „АЕЦ Козлодуй" ЕАД.

Изпълнителя да осигури обучение на минимум трима специалисти от персонала на Възложителя, за всяка една от функционалностите на системата за защита от кибератаки по предварително предоставена от Изпълнителя Програма за обучение.

Обучението да включва поредица лекции и практически, лабораторни упражнения, предназначени да предоставят на обучаваните необходимите умения и знанията за придобиване на умения за инсталиране, конфигуриране и поддръжка на всяка една от функционалностите налични в системата за защита от кибератаки.

При необходимост или по искане на Възложителя, в периода на гаранционната поддръжка, Изпълнителят следва да организира полудневни или целодневни сесии за трансфер на знания по изготвена от Изпълнителя и съгласувана с Възложителя програма, включваща като минимум следните дейности:

- консултации и анализиране на публикувани обновления и мнение относно тяхната

приложимост;

- консултации по работоспособността на функционалностите и услугите и производителността и натоварването на системата;
- съдействие при извършване на конфигурационни промени, свързани с нормалната експлоатация на системата или с промяна или добавяне на функционалности;
- преглед на промените през периода (ако такива са настъпили) и разглеждането в детайли на определени теми

Обемът на тези сесии да не е по-малък от 50 часа общо за гаранционния период и следва да бъде включен в ценовото предложение на Изпълнителя.

13.9. Необходими лицензии, разрешения, удостоверения, сертификати и др. на Изпълнителя.

13.9.1. Изпълнителят (ако не е производител), трябва да е оторизиран от производителя/ите или от негов официален представител да извършва доставка и поддръжка за цялото предложено оборудване и софтуер.

13.9.2. Изпълнителят трябва да осигури централизирана система за управление на поддръжката (help desk/service desk), в която се регистрират всички заявки, инциденти и проблеми на Възложителя. Системата трябва да поддържа като минимум следните канали за достъп и заявяване на услуги: E-mail; Телефон; Уеб-портал.

14. Гаранционни условия

Гаранционната поддръжка да е с минимална продължителност 3 години осигурена от производителя на оборудването и софтуера.

14.1. Гаранционното обслужване трябва да обхваща следните дейности на Изпълнителя:

- Отстраняване на проблеми при функционирането, дължащи се на дефекти в оборудването, неправилни настройки и конфигурации, вкл. при инсталирането му в инфраструктурата на Възложителя;
- Поддържане на лицензи и активни абонаменти за нови дефиниции версии съобразно договореното ниво

14.2. Параметрите на качеството на обслужване на доставеното оборудване са както следва:

- режим на приемане на заявки (по телефон, e-mail или регистриране на проблем в on-line система за сервизно обслужване на Изпълнителя) - поддържащ център (help desk) 24/7;
- време за реакция (потвърждаване на получена заявка) от момента на подаването ѝ за възникнал проблем - максимално 30 минути в работно време;
- време за възстановяване на функционалностите и услугите предоставяни с отдалечен достъп (независимо от характера на проблема) - до 1 работен ден;
- време за разрешаване на хардуерен проблем - максимално 3 работни дни;
- възможност за подмяна (ако периодът за ремонт е по-дълъг от допустимото време за решаването на проблема) на дефектните части или компоненти с част или компонент със същите или по-добри характеристики.

15. Контрол от страна на „АЕЦ Козлодуй” ЕАД

„АЕЦ Козлодуй” ЕАД има право да извършва инспекции и проверки на възложените за изпълнение дейности. Изпълнителят осигурява достъп до персонал, помещения, съоръжения, инструменти и документи, използвани от външните организации и техни подизпълнители.

С договора, Възложителят ще определи длъжностни лица от АЕЦ "Козлодуй" и техните отговорности във връзка с изпълнение му.

16. Организационни изисквания

16.1. Изпълнителят е длъжен да осигури за своя сметка присъствие на свой компетентен персонал на работните срещи и технически съвети, провеждани на площадката на АЕЦ "Козлодуй" , имащи отношение към изготвяния проект.

16.2. Изпълнителят е длъжен да изготви и спазва споразумение за безопасност и охрана на труда и поддържане на експлоатационния ред на площадката на АЕЦ "Козлодуй".

16.3. Разрешение за работа се получава от Възложителя, съгласувано с утвърдените план-графици, при изпълнение на условията на “Инструкция по качество. Работа на външни организации при сключен договор”, ДБК.КД.ИН.028.

17. Допълнителни изисквания

За изпълнение на дейностите по проектиране и внедряване на системата за защита от кибератаки, от Изпълнителя се изисква да притежава опит при внедряването на проекти за киберсигурност на информационни и комуникационни системи.

18. Изисквания към Изпълнителя при използване на подизпълнители/трети лица

При използване на подизпълнители/трети лица, основният Изпълнител по договора:

-носи отговорност за изпълнението на изискванията на ТЗ от подизпълнителите/трети лица за изпълняваните от тях дейности, както и за качеството на тяхната работа;

- определя линиите за комуникация и взаимодействие с неговите подизпълнители/трети лица и начините на контрол върху дейностите, които им са превъзложени и отговорните лица за изпълнение на този контрол;

- определя по подходящ начин и в необходимата степен приложимите изисквания на ТЗ за подизпълнители/трети лица по договора, в зависимост от дейностите, които изпълняват;

- определя като минимум изискванията си за СУ на подизпълнители/трети лица: необходимост от ПОК, приложими норми и стандарти, ред за управление на несъответствията, обем на документацията, изпитания и проверки и др.;

- съгласува ПОК на подизпълнителите/трети лица и представя съгласуваната ПОК за информация на „АЕЦ Козлодуй”ЕАД;

- включва в документацията на договора с подизпълнители/трети лица, всички определени по-горе изисквания.

Заличено на основание ЗЗЛД

РЪКОВОДИТЕЛ УПРАВЛЕНИЕ "ИНФОРМАЦИОН
И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ",
АЛЕКСАНДЪР ЗЛАТАНОВ