Техническа спецификация по обособена позиция № 6 с предмет:

„Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи“

1. Подсистема за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка

Общи изисквания	
REQ.1.	Брой на крайните точки: 8000
REQ.2.	Тип решение: 1 брой основен хардуер с вграден софтуер и 5-годишна поддръжка, 1 брой хардуер за DMZ с вграден софтуер и 5-годишна поддръжка, включени 8000 лицензи (софтуерни агенти) за поставяне на крайните точки, също с 5-годишна поддръжка, 5-годишен абонамент за прилежащи услуги към 8000-те агента
REQ.3.	Решението трябва да е споменато в документа на Gartner: Market Guide for Endpoint Detection and Response Solutions.
REQ.4.	Решението трябва да притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC).
REQ.5.	Решението да предоставя цялостна защита за крайни точки, включително засичане и превенция на атаки, да предоставя функции за разследване и почистване (в зависимост от метода на имплементация на решението), като да се поддържат минимално следните операционни системи на крайните точки: Window (XP, 7, 8, 10, Server 2003, 2008, 2012, 2016), mac OS X и Linux (RHEL, CentOS, Ubuntu, Suse).
REQ.6.	Решението трябва да включва специализирано устройство (хардуер), което да служи за централизирано управление на инсталираните агенти по крайните точки, за да могат да се наблюдават всички защитени крайни точки за съмнително зловредно поведение и да може да се извършва централизирано разследване.
REQ.7.	Агентите на решението трябва да могат да засичат, анализират и позволяват ответна реакция на напреднали кибератаки, използващи непознати „zero-day” уязвимости, независимо дали крайните точки се намират във или извън мрежата на организацията.
REQ.8.	Комуникацията между софтуерните агенти и централизираното управление трябва да е криптирана.
REQ.9.	Агентите на крайните точки трябва да са с малък размер, с минимално влияние на производителността на системите, като да се предоставя механизъм за контролиране на какъв процент от процесорната мощ на крайните точки да се използва за анализ и превенция на атаки, така че да не се влияе на нормалната работа на потребителите.
REQ.10.	Решението трябва да предоставя минимално следните функционалности: • Корелация в реално време на индикаторите за компроментиране на ниво крайна точка. • Засичане и блокиране на exploit атаки, използвайки алгоритми за анализиране на поведението на приложенията. Засичане на ROP (Return Oriented Programming) атаки, reverse shell, heap spray, SEHOP corruption, атаки използващи Java уязвимости.

	• Засичане на зловредни файлове в реално време. • Сканиране на файлове използвайки антивирусни алгоритми с дефиниции и чрез евристичен анализ. • Сканиране на изпълними файлове чрез алгоритми за машинно обучение (machine learning). • Възможност за сортиране на информация, за да може да се потвърди наличието на дадена атака и за да може да се възпроизведе целия ѝ жизнен цикъл за анализ. • Автоматично създаване на графика с хронолигично подредени събития, довели до компроментирането на дадена крайна точка. • Възможност за изключително бързо търсене в избрани крайни точки за зададени ключови думи, MD5 / SHA1 и SHA256 суми, сложни изрази, създадени файлове в зададен интервал от време, конкретни „бисквитки“, име на DNS хост, конкретни драйвери, файлови атрибути, HTTP хедъри, IP адреси, използвани портове за мрежова комуникация и активни процеси, конкретни ключове в регистрите на операционната система, Windows събития. • Фунцкията за търсене на информация трябва да може да се използва директно от графичния интерфейс на решението, както и използвайки API интерфейс, така че да могат да се използват автоматизирани скриптове. • Да могат да се изолират заразените крайни точки директно от централизираното управление на решението (по заявка от администратор), позволявайки им комуникация само с посочени IP адреси (Endpoint containment).
REQ.11.	Решението трябва да може автоматично да събира и да предоставя информация за използвани уязвимости, процеси, домейни, регистри, файлове и мрежова активност за вдигнатите аларми. Информацията трябва да е достъпна за преглед директно от графичния интерфейс на конзолата за централизирано управление.
REQ.12.	Решението трябва да позволява извличането на файлове от системите, на които има инсталиран агент. За Windows операционни системи, решението трябва да може да извлича заключени или изтрити файлове, ако те все още не са презаписани от нова информация.
REQ.13.	Решението трябва да позволява извличането на файлове, които са записани на крайните точки в следствие на зловредна активност, директно от интерфейса за разследване на аларми на централизираното управление.
REQ.14.	Фунцкията за извличане на файлове трябва да може да се използва директно от графичния интерфейс на решението, както и изпозлвайки API интерфейс, така че да могат да се използват автоматизирани скриптове.
REQ.15.	Решението трябва да може автоматично да генерира пакети с данни от крайните точки (endpoint triage), за да се подпомогне разследването на аларми. Пакетите с данни трябва да съдържат информация за системните параметри на крайната точка, процесите, файловете, регистрите, потребителските акаунти, история на браузването.
REQ.16.	Решението трябва да позволява извличането на информация за подпомагане на разследванията, като историята на извиканите shell команди, цялото дисково пространство на

	дадена крайна точка, цялата информация от паметта на крайната точка, историята на извиканите powershell команди, списък на процесите в паметта, списък на файловете на дисковото пространство на крайната точка.
REQ.17.	Решението трябва да може да получава индикатори за компроментиране директно от производителя и от другите подсистеми за киберсигурност, както и да се позволява създаването на собствени индикатори за компроментиране от администраторите, също така да е възможна и интеграцията с външни източници на индикатори.
REQ.18.	Решението трябва да позволява наблюдението на крайни точки и засичане на вируси тип троянски кон, червеи, шпионски софтуер, adware, key logger вируси, rootkit вируси и exploit вируси, които се появяват след употребата на приложения като например Adobe Reader, Adobe Flash, Internet Explorer, Firefox, Google Chrome, Java, Microsoft Outlook, Microsoft Word, Microsoft Excel и Microsoft PowerPoint, включително да могат да се блокират и спират от агента заразените приложения.
REQ.19.	Решението трябва да може да изпраща файлове за по-нататъшен анализ към подсистема за sandbox анализ, разположена локално в структурите на организацията (on premise).
REQ.20.	Решението трябва да може да следи изпълнението на файлове, като да може да определи дали са изпълнени за първи път или пътя на изпълнение на файловете е променен. Тази информация (мета данни) трябва да може да се изпраща към решение тип SIEM чрез интеграция.
REQ.21.	Решението трябва да може да засича непознати „zero-day" атаки, като динамичния анализ на поведението на процесите трябва да работи минимално за .dll, .ocx, .sys и изпълними (.exe) файлове, като анализа да се извършва локално, без да е необходимо изпращането на проби към облачни услуги или трети OEM решения.
REQ.22.	Агентите на решението трябва да могат да записват локално събитията свързани с работата с файлове (създаване, отваряне, модифициране), с мрежовите комуникации от крайните точки, DNS заявките, достъпените URL адреси, стартираните процеси, с използваните ключове от регистрите на операционната система.
REQ.23.	Решението трябва да позволява да се изолират заразените крайни точки директно от централизираното управление на решението (по заявка от администратор), позволявайки им комуникация само с посочени IP адреси (Endpoint containment), така че да се спре разпространението на заразата по мрежата. Механизма трябва да позволява използването на различни роли на потребителите, които да правят заявки за изолиране на заразена крайна точка и които да одобряват заявките.
REQ.24.	Решението трябва да може централизирано да обновява софтуерната версия на инсталираните агенти.
REQ.25.	Решението трябва да разполага с механизми за собствена защита от спиране или рестартиране на инсталираните агенти, както и от инжектиране на нежелани процеси в тях.
REQ.26.	Решението трябва да предоставя механизъм с използване на парола, за да се предотврати премахването на инсталиран агент от неоторизирано лице.
REQ.27.	Решението трябва да разполага с добре описан API интерфейс за интегриране.

REQ.28.	Решението трябва да позволява администрация чрез уеб-базирана конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ.
REQ.29.	Решението трябва да позволява използването на прокси с оторизация за свързване със сървър за обновления на софтуера и информацията за нови заплахи.
REQ.30.	Решението трябва да може да създава, съхранява и предоставя log файлове към трети решения, използвайки Syslog протокол, например за предоставяне на информация на решения от тип SIEM.
REQ.31.	Решението трябва да позволява интеграция с решения тип SIEM за автоматична подмяна на заявки и информация, така че да се намали необходимото време за разследване на атака.
REQ.32.	В случаите когато агента не може да установи комуникация с устройстовто-контролер, агента трябва да продължи нормалната си работа и да изпрати събраната информация към контролера, когато комуникацията се установи отново.
REQ.33.	Решението трябва да може да се интегрира с подсистемата за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения за корелация на събития през подсистемата за централизирано управление.
Хардуерни изисквания – 2 броя основен и DMZ	
REQ.34.	Устройството да може да управлява сигурността на до 100 000 крайни точки (максимален капацитет на скалируемост)
REQ.35.	Устройството да е с максимална големина 1U
REQ.36.	Устройството да разполага с ефективно място за съхранение на получените данни от крайните точки, минимално 8TB
REQ.37.	Устройството да разполага минимално със следните портове: 2x 1GigE BaseT, 1x IPMI, 2x USB3 (rear), 1x DB9 Serial, 1x VGA
REQ.38.	Резервирано захранване – 1+1
REQ.39.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция и поддръжка:	
REQ.40.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.41.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.42.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.43.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

2. Подсистема за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения

Общи изисквания	
REQ.44.	Брой пощенски кутии: 8000
REQ.45.	Тип решение: 2 броя хардуер (High-Availability) с вграден софтуер и 5-годишна поддръжка, както и включен абонамент за 8000 софтуерни лицензи за анализиране на прикачени файлове и URL

	адреси в email съобщенията, също с 5-годишна поддръжка, 2 бр. 5-годишен абонамент за прилежащи услуги към хардуерните устройства
REQ.46.	Решението трябва да може да открива и идентифицира зловреден код, който е скрит и влиза в организацията чрез електронната поща, като трябва да се използват технологии и методи за засичане, които да не са базирани само на статичен анализ чрез дефиниции, статични списъци или правила, а да може да извършва и динамичен анализ и да открива непознати “zero-day” заплахи.
REQ.47.	Решението трябва да се предоставя под формата на специализиран хардуер, като производителя трябва да е отговорен и да предостави лицензи за софтуер за поне 120 виртуални машини за анализ, с прилежащите им операционни системи и приложения.
REQ.48.	Решението трябва да притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC).
REQ.49.	Решението трябва да може да открива фишинг и spear-фишинг атаки. Трябва да може да анализира прикачени файлове и URL адреси в електронните съобщения, за да открива опити за компроментиране на системите на организацията.
REQ.50.	Решението трябва да може да открива impersonation атаки (представяне с чужда самоличност). Трябва да се позволява конфигурирането на отношения между имена и email адреси, така че да се засичат опити за impersonation атаки, които копират имената или email адресите на потребителите.
REQ.51.	Решението трябва да може да засича зловреден код с голяма точност, с изключително малък процент на грешни показания. Трябва да може да се открива с точност зловреден код, независимо от MIME тип, тип на разширение (extension) и независимо дали са използвани техники за скриване или архивиране на съдържанието на електронните съобщения.
REQ.52.	Решението трябва да може да поставя в карантина email съобщения, които съдържат URL адреси в тялото си, съдържат MS Office документи, PDF документи, архиви и HTML файлове, замаскирани JAVA скриптове, замаскирани, съкратени или пренасочващи URL адреси.
REQ.53.	Решението трябва да може да разпознава заплахи като извършва локален анализ, без да е необходимо да изпраща файлове, проби от зловреден код или изпълним код извън организацията или към облачно-базирани платформи за анализ.
REQ.54.	Решението трябва да може да анализира множество типове файлове, използвайки различни приложения и техни версии за анализа, съответно за разширения (минимално): exe, dll, pdf, pub, doc, docx, xls, xlsx, js, gif, jpeg, png, tiff, swf, eml, mov, qt, mp4, jpg, mp3, asf, ico, htm, hta, url, rm, com, vcf, ppt, rtf, chm, hlp.
REQ.55.	Решението трябва да може да извлича и анализира вмъкнати файлове в документи, като например pdf, rtf или MS Office документи.
REQ.56.	Решението трябва да може да поставя в карантина и да алармира за криптирани MS Office документи.
REQ.57.	Решението трябва да може да поставя в карантина и да алармира за прикачени MS Office документи, които съдържат макроси или имат вградени в тях документи, независимо от резултата от анализа.

REQ.58.	Решението трябва да може да поставя в карантина и да алармира за електронни съобщения, които съдържат в себе си съкратени URL адреси.
REQ.59.	За електронни съобщения, които съдържат URL адреси, които водят до сваляне на файлове, решението трябва да може да извлича и анализира въпросните файлове от URL адресите, като да може да се блокира съобщението ако файловете се окажат зловредни.
REQ.60.	Решението трябва да може да поставя в карантина и да алармира за електронни съобщения, които съдържат прикачени JAR файлове или съдържат URL адреси, които водят до JAR файлове.
REQ.61.	Решението трябва да може да извлича и анализира URL адреси от съдържанието на електронните съобщения и от секцията „Относно“ на съобщенията, както и от прикачени PDF или MS Office документи.
REQ.62.	Решението трябва да може да засича следните техники, които се използват от атакуващите хакери, за да подмамят потребителите да достъпят конкретни URL адреси: заместване на знак от адреса с друг (typosquatting), използване на линк към различен адрес от изобразения (URL overlay).
REQ.63.	Решението трябва да може да анализира URL адреси от тип ftp, http и https.
REQ.64.	Решението трябва да може да анализира base64 кодирани URL адреси.
REQ.65.	Решението трябва да анализира прикачени архиви тип 7Z, ZIP, LZH, RAR. Ако архивите са защитени с парола, решението да може автоматично да търси подходящи варианти за парола в съдържанието на електронното съобщение, в самите файлове-архиви или в прикачени изображения към съобщението чрез OCR технология.
REQ.66.	Решението трябва да може да извлича и анализира URL адреси от заключени с парола PDF или MS Office документи. Решението да може автоматично да търси подходящи варианти за парола в съдържанието на електронното съобщение или в прикачени изображения към съобщението чрез OCR технология (изображения тип JPEG, PNG, BMP, TIFF).
REQ.67.	Решението трябва да може да анализира файлове не само чрез статичен анализ с дефиниции, но и чрез алгоритми за машинно обучение и динамичен анализ тип sandbox.
REQ.68.	Решението трябва да може да анализира (във виртуалните машини за динамичен анализ) свалените файлове от заявки идващи от exploit атаки. Например, ако прикачен файл към електронно съобщение съдържа скрипт / макрос, който опитва да свали допълнителни файлове и съдържание, то решението трябва да може успешно да ги свали и анализира, за да се открият и предотвратят атаки, които се развиват на няколко фази.
REQ.69.	Решението трябва да може да открива с много висока точност, с възможно най-малко грешни показания, файлове, които след анализ на поведението се държат по подобие на зловреден код: поведение, което опитва да избегне засичане, инсталиране на нежелани програми, промени по системните настройки, намаляване на цялостната производителност на системата, потенциално нежелани програми (PUP), потенциално нежелани приложения (PUA), adware процеси, инструменти, които често се използват от атакуващи хакери.
REQ.70.	По време на анализа във виртуалните машини, решението трябва да може да извлича и анализира URL адресите в паметта на машините.

REQ.71.	Решението трябва да може да засича ransomware криптиращи атаки и атаки предназначени за POS терминали.
REQ.72.	Решението трябва да може да алармира за зловредни процеси (файлове и URL адреси), които не са били засечени в първоначалните 24 часа, а на по-късен етап е установено, че са зловредни.
REQ.73.	Решението трябва да предоставя цялостна информация след анализ на зловреден код. Информацията трябва да включва използвани уеб линкове за атаката, хеш суми на свалените файлове, цялостен одит на действията по системите (променени ключове от регистрите, създаване и изпълнение на файлове, промяна в автоматичните настройки и параметрите за стартиране на приложения), както и да се предоставя информация за хронолигчния ред от събития, свързани с атаката, започващи от фазата на уеб-експлоатация и първоначално проникване, до свалянето на код, установяване на контрол над системите и опитите за извличане на данни извън организацията.
REQ.74.	Решението трябва да предоставя следствена информация след динамичния анализ на файлове, представена в графичен вид, изобразявайки процеси, достъпи до паметта, промени по файлове и регистри, качени DLL библиотеки, инжектиране на код, heap spraying процеси, mutex процеси.
REQ.75.	Решението трябва да може да предоставя, където е възможно, информация за атакуващата хакерска групировка и възможни стъпки за отстраняване на щетите (remediation) след дадена атака.
REQ.76.	Ако при анализ на зловреден прикачен файл се установят опити за мрежови свързвания извън организацията от него, решението трябва да сигнализира и за тях при вдигането на съответната аларма.
REQ.77.	Решението трябва да може да предоставя screenshot на зареден в браузър зловреден URL адрес по време на анализа му, за да се добие визуална представа за съдържанието на URL адреса.
REQ.78.	Решението трябва да може да прави корелация на електронни съобщения със сходни характеристики, като например с еднакви прикачени файлове, еднакви заглавни части, еднакви изпращачи и т.н. и да може да ги групира като email кампании.
REQ.79.	Решението трябва да може да прави анализ на входящи електронни съобщения, използвайки едновременно множество виртуални машини с различни операционни системи, като например минимално Windows XP, 7 или Mac OSX, с различни версии на Service Pack, на 32 и на 64 битови платформи.
REQ.80.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н. Решението трябва да използва собствен, специално изграден хипервайзор.
REQ.81.	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция,

	историята от браузването, използваният Outlook акаунт, езика на машината, времевата зона на машината.
REQ.82.	Решението трябва да може да засича опити за използване на функциите за приспиване (sleep) на операционните системи от зловредния код и да може да забързва времето на виртуалните машини за анализ, за да принуди изпълнението на зловредния код.
REQ.83.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques), например използване на ping команди, проверка на домейн, проверка на отметки в наличните браузъри.
REQ.84.	Email решението трябва да поддържа inline MTA режим на работа.
REQ.85.	Email решението трябва да поддържа SPAN/TAP режим на работа.
REQ.86.	Email решението трябва да поддържа BCC режим на работа.
REQ.87.	Решението трябва да позволява (по избор от администратор) извършване на динамичен анализ на файлове във виртуалните машини, както в режим на изолация (без да е необходима свързаност с Интернет), така и с позволено мрежово свързване от виртуалните машини, за да се добие цялостен анализ на зловредния код.
REQ.88.	Решението трябва да използва специално заделен мрежови интерфейс когато е пуснато в „жив“ режим, за да се избегне допускането на зловреден мрежови трафик към реалната вътрешна мрежа на организацията; Мрежовия интерфейс трябва да позволява на зловредния код да достъпва външни хакерски командни сървъри и да сваля всички допълнителни модули и артефакти, които са му необходими, за да се изпълни изцяло за анализ.
REQ.89.	Решението трябва да може да симулира потребителски действия, за да изпълни зловреден код изискващ подобни действия, като например щракане с мишката или конфигуриране на конкретни данни.
REQ.90.	Цялостния анализ на електронно съобщение не трябва да отнема повече от 10 минути.
REQ.91.	Решението трябва да позволява на администраторите да конфигурират максималното време за анализ на електронните съобщения.
REQ.92.	Решението трябва да позволява използването на YARA правила и да позволява конфигурирането на автоматични аларми или поставяне в карантина ако дадено съобщение отговаря на зададените YARA правила.
REQ.93.	Решението трябва да може да засича и отчита опити за мрежова комуникация с Интернет от виртуалните машини по време на анализа.
REQ.94.	Решението трябва да позволява на администраторите да посочват и обвързват с кои приложения да се стартират различните файлови разширения по време на анализа във виртуалните машини.
REQ.95.	Решението трябва да може да се имплементира в различни режими, както „Inline”, на пътя на трафика, с възможност за блокиране, така и „Out-Of-Band“, където да се анализират копия на електронните съобщения.
REQ.96.	Решението трябва да може да работи в напълно изолирана среда, без връзка с Интернет.
REQ.97.	Решението трябва да може да изпраща автоматични известия чрез Syslog, HTTP, SNMP и SMTP протоколи.

REQ.98.	Решението трябва да поддържа криптирана TLS комуникация (opportunistic или imposed), за да се запази конфиденциалността на електронните съобщения.
REQ.99.	Решението трябва да може да изпраща автоматични известия когато блокира или постави в карантина дадено електронно email съобщение.
REQ.100.	Решението трябва да позволява конфигурирането на обема на заделеното място за карантина на съобщенията и да може да изпраща автоматични известия когато заделеното пространство се запълни до определен процент.
REQ.101.	Решението трябва да позволява използването на прокси с оторизация за свързване със сървър за обновления на софтуера и информацията за нови заплахи.
REQ.102.	Решението трябва да позволява администрация чрез уеб-базирана конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ.
REQ.103.	Решението трябва да позволява конфигурирането на ACL списъци, за да се ограничи достъпа до интерфейса за централизирано управление.
REQ.104.	Решението трябва да използва криптирана комуникация между администраторите и конзолата за централизирано управление. Трябва да позволява вмъкването на собствени дигитални сертификати на организацията.
REQ.105.	Решението трябва да позволява локално конфигуриране или чрез синхронизация с NTP сървър на използваните време и часова зона.
REQ.106.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление. Да могат да се задават различни профили и права (администратор, оператор, одитор и т.н.), като да се задават кои отчети, аларми и информация могат да виждат в конзолата за управление.
REQ.107.	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите.
REQ.108.	Решението трябва да може да изпраща известия за собственото си здраве и процеси и генерираните отчети, чрез SMTP, SNMP и Syslog протоколи.
REQ.109.	Решението трябва да позволява извличането на аларми и отчети за активност на зловреден код в PDF формат.
REQ.110.	Решението трябва да позволява групирането на аларми за зловредни email съобщения по поне следните критерии: по изпращачи, по получатели, по видове вдигнати аларми, по email кампания.
REQ.111.	Решението трябва да позволява генерирането на отчети в PDF или в CSV формат, според типа информация в тях: вдигнати аларми и техните детайли, тип инфекция, обобщителна информация за предоставяне пред ръководните органи на организацията, списък с достъпените сървъри при callback комуникация и други.
REQ.112.	Решението трябва да предоставя опция да получава и изпраща обекти за анализ, когато бъде достигнат зададен лимит на капацитета на обработваните обекти от решението, към предварително зададен локално-разположен клъстър или към специализирани хардуерни устройства за балансиране на производителността.

REQ.113.	Решението трябва да позволява извличането на метаданни от email съобщенията, минимално получател, прикачени файлове и вмъкнати URL адреси, като тези метаданни да могат да се изпращат към решение тип SIEM, чрез HTTP или чрез Rsyslog протокол.
Хардуерни изисквания – 2 броя	
REQ.114.	Устройството да може да анализира до 2650 уникални прикачени файлове към email съобщения в час
REQ.115.	Устройството да може да анализира прикачени файлове и URL адреси в email съобщенията за 8000 пощенски кутии
REQ.116.	Устройството да е с максимална големина 2RU
REQ.117.	Устройството да разполага минимално със следните портове за наблюдение на мрежата: 2x 1GigE BaseT
REQ.118.	Допълнителни портове: 2x 1GigE BaseT портове за управление, сериен порт, 4x Type A USB, IPMI, VGA
REQ.119.	Резервирано захранване – 1+1
REQ.120.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция и поддръжка:	
REQ.121.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.122.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.123.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.124.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

3. **Подсистема за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво**

Общи изисквания	
REQ.125.	Тип решение: 2 броя хардуер (High-Availability) с вграден софтуер и 5-годишна поддръжка, с добавени 2 броя разширителни модули тип 1G-10G BASE-LX/LR FIBER, 2 бр. 5-годишен абонамент за прилежащи услуги към хардуерните устройства
REQ.126.	Предложеното решение трябва да може да инспектира и блокира зловреден мрежови трафик като да се поставя на пътя на трафика в inline режим или в „out-of-band“ режим, като да може да работи независимо от останалото мрежово оборудване в инфраструктурата.
REQ.127.	Решението трябва да притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC).
REQ.128.	Решението да поддържа режим на работа с висока достъпност - high availability (HA), от типа active-active.
REQ.129.	Решението трябва да може да функционира независимо от което и да е друго мрежово устройство (например защитни стени, IDS/IPS устройства, security gateway устройства и т.н.). Решението трябва да е специализирано и да може да работи самостоятелно, като функциите му не трябва да са част от UTM или интегрирано решение за сигурност.

REQ.130.	Предложеното решение трябва да предоставя предварително зададени правила за разпознаване на зловредни мрежови действия от приложенията, разположени по работните станции и сървърите в инфраструктурата на организацията. Трябва да има възможност за обновяване на тези правила използвайки актуална информация събрана от вендора за най-новите заплахи.
REQ.131.	Решението трябва да може да анализира мрежови трафик от организацията към Интернет и да засича изпълнението на нежелани приложения или callback комуникации с хакерски командни центрове, като по тази начин да могат да се блокират опити за изнасяне на информация извън организацията по мрежата, като или да се блокира мрежовата сесия ако се работи в inline режим или като вгражда „reset“ пакети в комуникацията ако се работи в „out-of-band“ режим.
REQ.132.	Решението да може да функционира като ICAP сървър, като да може да получава файлове за анализ чрез ICAP протокола.
REQ.133.	Решението трябва да може да засича ранните фази на уеб-базираните атаки, например първоначално стартиране на exploit, сваляне на зловреден бинарен код, callback функции и комуникации с хакерски командни центрове, за да може да идентифицира уязвимости в системите и приложенията на организацията, за да може да засича заразени системи и за да може да блокира неоторизирани комуникации навън от средата, по няколко мрежови протокола.
REQ.134.	Предложеното решение трябва да може да инспектира и да открива зловредни обекти, зловредни URL мрежови адреси и зловредни действия в поне следните мрежови протоколи: HTTP, HTTPS, FTP, SMB.
REQ.135.	Предложеното решение трябва да може да засича движение на атаките „настрани“ в организацията (lateral spread) като анализира SMB, WinRM и MS-SQL трафик и да може да засича и алармира за дейности след успешен exploit на уязвимости от атакуващите, от вътрешна работна станция до вътрешен трафик (трафик тип изток-запад), като например вътрешно разузнаване, ескалиране на права за достъп на акаунти, извличане на потребителски имена и пароли, движение „настрани“ на зловреден код, изпълнение на дистанционни команди, извличане на данни.
REQ.136.	Предложеното решение трябва да е под формата на специализирано хардуерно устройство и вендора трябва да предостави пълни лицензи за софтуера, който ще се използва от устройството за анализиране на зловреден код, както и необходимите лицензи за операционните системи и приложенията, използвани от виртуалната среда за анализ на кода.
REQ.137.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.
REQ.138.	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, използваният Outlook акаунт, езика на машината, времевата зона на машината.

REQ.139.	Решението трябва да предоставя среда за динамичен анализ, която да се състои от предварително създадени виртуални машини, които да са изцяло предоставени и поддържани от вендора на решението, за да се избегне сложността произтичаща от инсталирането на приложения и поддръжката на виртуални машини от страна на организацията.
REQ.140.	Решението трябва да може да идентифицира атаки, без да внася забавяне в мрежовия трафик на организацията, като анализа трябва да се извършва локално, на мрежовото ниво, където е разположено устройството.
REQ.141.	Решението трябва да има механизъм за класифициране и поставяне на етикети на бинарен код на машинно ниво, които се отнася за EXE, DLL и SYS файлове.
REQ.142.	Предложеното решение трябва да дава възможно най-малко грешни показания и да вдига възможно най-малко грешни аларми при засичането на файлове, които наподобяват зловреден код: да алармира за поведение, което опитва да избегне засичане от системите за сигурност, инсталиране на нежелани програми, промяна на системните настройки, което влошава производителността на системите, наличие на потенциално нежелани програми (PUP) и на потенциално нежелани приложения (PUA), adware процеси и използване на инструменти, които често се използват от атакуващи хакери.
REQ.143.	Решението трябва да може да разпознава заплахи чрез извършване на локален анализ, без да се изпращат файлове, проби от кода или изпълним код извън организацията или към облачно-базирани системи за анализ.
REQ.144.	Трябва да има възможност за комплексно разследване за целия цикъл на атаките, включително върху всяка от следните фази, за които да има отделни аларми: • Първоначално разпознаване на мрежата (Картографиране на мрежата, преброяване на хостовете, преброяване на услугите, издирване на потребителски акаунти); • Изпълнение (използване на командата „AT“ за насрочване на изпълнение на процеси, „pass-the-hash“ дистанционно изпълнение на код (RCE), използване на инструментариума за управление на Windows средите (WMI), дистанционно създаване на процеси); • Изпълнение на Web Shell; • Сваляне на зловреден код (malware); • Извличане на информация чрез свързвания с хакерски команден сървър; • Разпространяване на зловредния код (трансфер на зловреден код чрез SMB и SMB 2 протоколи) • Ескалиране на привилегии (преброяване на групите с високо ниво на достъп, преброяване на дистанционно споделените ресурси - remote shares) • Извличане на данни за вписване в системите (трансфер на пароли чрез SMB протокол, извличане чрез Mimikatz, извличане на NTLM хешове) • Дистанционно изпълнение на процеси.
REQ.145.	Решението трябва да може да идентифицира уеб-базирани уязвимости, чрез извършване на анализ на съмнително уеб съдържание във виртуалните машини за анализ, използвайки същия тип браузър, както реалния потребител достъпил уеб съдържанието.

REQ.146.	Решението трябва да може да засича атаки към сървърите като извлича и анализира статични и динамични уеб-базирани файлове (PHP, WAR, JSP, ASP, ASPX), които са качени на уеб сървърите чрез HTTP POST или FTP.
REQ.147.	Решението трябва да предоставя детайлна информация за аларми, произлизащи от извлечените метаданни от транспортния и от приложния слой на мрежата, за поне следните протоколи: FTP, HTTP, IMAP, IRC, POP3, RDP, RTSP, SIP, SMB, SMTP, SSH, TLS; Решението трябва да може да визуализира метаданните в интерактивна, графична форма, както и да позволява извличането им за интегриране с трети SIEM решения.
REQ.148.	Решението трябва да може да инспектира HTTPS трафик, като да се поддържат SSL / TLS протоколи, включително да се поддържат функции като JA3 fingerprinting, използване на „бели списъци“ и URL категоризация.
REQ.149.	Решението трябва да може да анализира поне следните файлови типове: msi, exe, dll, pdf, doc, chm, avi, jar, docx, xls, xlsx, gif, jpeg, png, tiff, swf, swf embedded in swf, scr, mov, qt, mp4, jpg, mp3, asf, ico, htm, hta, url, rm, com, vcf, ppt, rtf, chm, hlp и други.
REQ.150.	Решението трябва да предоставя „предварителен изглед“ на засечените съмнителни URL адреси, като да може да предоставя на анализаторите screenshot-и от URL адресите.
REQ.151.	Решението трябва да може да извършва динамичен анализ за зловреден код, да може да се обновява и да може да му се предоставя нова информация за заплахи, дори в offline режим, без да има връзка с Интернет.
REQ.152.	Решението трябва да може да предоставя контекстуална информация към вдигнатите аларми, като например източник, степен на опасност, потенциални рискове, варианти за справяне с проблема и т.н., за засечените атаки от дадена рискова група.
REQ.153.	Решението трябва да разполага с голям набор от виртуални машини за sandbox анализ, с предварително инсталирани операционни системи и софтуер, бивайки Windows OS (включително XP, 7, 10), Mac OSX и Linux Cent OS, с различни версии на Service Pack, 32 и 64 битови, за да може да извършва точен анализ на поведението на процесите според различните уязвимости на средите.
REQ.154.	Решението трябва да предоставя множество приложения с различни версии за тестове, разположени на виртуалните машини за анализ на зловредни файлове. Приложенията и версиите трябва да бъдат минимум следните: Microsoft Office 2003, 2007, 2010, 2013; Adobe Reader 7, 8, 9, 10, 11; Internet explorer 6, 7, 8, 9, 10, 11.
REQ.155.	Решението трябва да може да анализира един и същ файл на различни видове и версии на операционни системи и приложения, както и на различни версии на Internet Explorer, за да се открие потенциално зловредно поведение използващо конкретни уязвимости.
REQ.156.	Решението трябва да може да алармира за зловредни процеси, които не са били засечени в първоначалните 24 часа, а на по-късен етап е установено, че са зловредни.
REQ.157.	След извършване на анализ, решението трябва да може да предоставя пълен отчет за него, който да съдържа минимално следната информация: • Тип на анализираните файлове; • Име на пробата;

	• Контролните суми на анализираните файлове (MD5, SHA1 / 256/512); • Класификация според това към кое семейство се причислява засечения зловреден код; • Тип на използваната уязвимост за пробив; • URL адреси, които са използвани за атаката, както и предоставяне на информация за преглед на съдържанието на URL адресите чрез изображения (screenshots); • Данни за идентифициране на заразените системи (IP, MAC); • Графично изобразяване на поведението на анализирания зловреден код; • Извършени промени по операционните системи; • Извършени промени по инсталираните приложения на виртуалните машини за анализ; • Извършени промени по файловата система; • Извършени промени по регистрите на Windows операционните системи; • Качените DLL библиотеки; • Извиканите Windows API функции, в хронологичен ред; • Информация за създадените / модифицираните / спрените процеси; • Детайлно изобразяване на поведението на процесите на мрежово ниво в графичен формат (изпълнени мрежови свързвания и използваните транспортни мрежови протоколи, използвани портове, DNS заявки и отговори, http пакети); • Информация за IP адресите, с които е комуникирано;
REQ.158.	Решението трябва да може да съхранява данните от изпълнението на зловреден код и прилежащите артефакти, като например PCAP файл с данни от засечените заплахи, за да може информацията да се анализира допълнително и след извършения sandbox анализ.
REQ.159.	Решението трябва да може да се поставя в следните режими на работа: SPAN, TAP, inline или HW bypass.
REQ.160.	Решението трябва да позволява използването на YARA правила.
REQ.161.	Решението трябва да може да анализира мрежови трафик независимо от използваните VLAN и портове, без да изисква предварително задаване на параметри, включително да се поддържат протоколи Encapsulated remote SPAN, Virtual Extensible LAN и Internet Content Adaptation Protocol.
REQ.162.	Решението трябва да разполага с команден и с графичен интерфейс (достъпен през стандартен уеб-браузър) за централизирано управление, без да се изисква инсталиране на допълнителен софтуер.
REQ.163.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление. Да могат да се задават различни профили и права (администратор, оператор, одитор и т.н.), като да се задават кои отчети, аларми и информация могат да виждат в конзолата за управление.
REQ.164.	Решението трябва да може да анализира и засича атаки, които протичат на няколко нива и фази, а да не предоставя само sandbox технология за анализ на отделни файлове в изолация.
REQ.165.	Решението трябва да борави с различни версии на Microsoft Office във виртуалните машини за анализ, като да може да анализира Microsoft Office документи с вграден зловреден код или макроси за пароли, анализ на зловреден трафик от тях, както и да се засичат системни грешки свързани с документите.

REQ.166.	Решението трябва да може да засича и класифицира следните категории атаки: • Ransomware криптиращи атаки; • Следи от meterpreter команди; • Кражба на файлове; • Инфектиране на файлове; • Опити за силово разбиване на пароли; • Изпълнение на команди; • Използване на уязвимости за пробив (exploit); • Атаки с цел разузнаване;
REQ.167.	Решението трябва да може да анализира причините за принудително спиране на дадено приложение.
REQ.168.	Решението трябва да може да получава информация за нови киберзаплахи от глобална система за информация на производителя.
REQ.169.	Решението трябва да може да получава системни обновления и обновления за виртуалниите машини за анализ, директно от уеб-базирания интерфейс за централизирано управление на решението.
REQ.170.	Решението трябва да предоставя информация за системните си показатели в графичния интерфейс за управление.
REQ.171.	Решението трябва да позволява използването на прокси сървър с оторизация за сваляне на обновления.
REQ.172.	Решението трябва да може с точност да идентифицира и обособи филтриран и блокиран мрежови трафик през уеб прокси.
REQ.173.	Решението трябва да позволява филтриране на мрежови трафик, да се определя дали да се анализира или блокира трафика, като се използват „бели списъци“. Трябва да може да се филтрира на базата на: Generic Routing Encapsulation, използвани портове за комуникация и филтриране на конкретни мрежи (по зададени IP адреси или подмрежи).
REQ.174.	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите.
REQ.175.	Решението трябва да може да използва XFF хедъри за идентифициране на коя машина генерира аларми, когато се намира зад прокси сървър.
REQ.176.	Решението не трябва да позволява мрежова комуникация от виртуалните машини за анализ към Интернет и от анализирания зловреден код към хакерски команден център или към URL адрес.
REQ.177.	По време на извършван анализ, ако зловредния код изпрати заявка за сваляне на допълнителни файлове (двоичен код), решението трябва да може да предостави на виртуалната машина заместващ доброкачествен файл, за да се продължи изпълнението и анализа.
REQ.178.	Решението трябва да може да предоставя следната информация: • Доклад с промените по системите; • Копие на зловредния двоичен код;

	• Мета данни от зловредния код; • Уловен мрежови трафик (PCAP файл) от виртуалните машини за анализ; • Пълно описание на достъпените URL адреси от зловредния код с идентифицирне на локациите им.
REQ.179.	Решението трябва да може да предоставя извличането на отчети и аларми в PDF формат.
REQ.180.	Решението трябва да може да определи степента на заплаха на даден инцидент от вдигнатите аларми за него.
REQ.181.	Решението трябва да може да вдига различни аларми за всяка фаза от жизнения цикъл на засечените атаки.
REQ.182.	Решението трябва да може да засича опити за използване на функциите за приспиване (sleep) на операционните системи от зловредния код и да може да забързва времето на виртуалните машини за анализ, за да принуди изпълнението на зловредния код.
REQ.183.	Решението трябва да може да симулира потребителски действия, за да изпълни зловреден код изискващ подобни действия, като например щракане с мишката или конфигуриране на конкретни данни.
REQ.184.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques), например използване на ping команди, проверка на домейн, проверка на отметки в наличните браузъри.
REQ.185.	Решението трябва да може да изпраща известия за собственото си здраве и процеси, на базата на SMTP, до предварително зададени локации.
REQ.186.	Решението трябва да може да се интегрира (за обмен на информация) с подсистемата за улавяне на мрежови пакети, разследвания и централизиран анализ и визуализация, с подсистемата за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка и с подсистемата за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения.
REQ.187.	Решението трябва да предоставя опция да получава и изпраща обекти за анализ, когато бъде достигнат зададен лимит на капацитета на обработваните обекти от решението, към предварително зададен локално-разположен клъстър или към специализирани хардуерни устройства за балансиране на производителността.
Хардуерни изисквания – 2 броя	
REQ.188.	Производителност мрежова защита, мрежови трафик: минимално 2.4 Gbps
REQ.189.	Производителност на вградена IPS функционалност, мрежови трафик: минимално 2.4 Gbps
REQ.190.	Минимален брой поддържани едновременни сесии за IPS: 1M
REQ.191.	Минимален брой поддържани нови сесии в секунда за IPS: 20K/Sec
REQ.192.	Устройството да е с максимална големина 2RU
REQ.193.	Устройството да разполага с поне 4TB за съхранение на данни
REQ.194.	Устройството да разполага минимално със следните портове за наблюдение на мрежата: 8x 10GigE SFP+; 4x 1GigE Bypass и 2 допълнителни разширителни модула x 1G-10G BASE-LX/LR FIBER

REQ.195.	Устройството да поддържа следните режими на работа на портовете за наблюдение на мрежата: In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN
REQ.196.	Допълнителни портове: 2x 1GigE портове за управление, сериен порт, 4x Type A USB, IPMI, VGA
REQ.197.	Резервирано захранване – 1+1
REQ.198.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция и поддръжка:	
REQ.199.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.200.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.201.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.202.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

4. **Подсистема за централизирано управление**

Общи изисквания	
REQ.203.	Тип решение: 1 брой хардуер с вграден софтуер и 5-годишна поддръжка
REQ.204.	Решението трябва да може да извършва корелация на аларми между подсистемата за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво и подсистема за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения, както и подсистемата за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка, за да се предостави защита от атаки, които се изпълняват на няколко нива и през няколко вектора. Например: атака чрез зловреден URL адрес, предоставен чрез съдържанието на електронно email съобщение, с прилежащ свален през уеб трафик зловреден файл, който е изпълнен на крайна точка, довело до нейното заразяване.
REQ.205.	Решението трябва да може да предоставя и изпълнява обновления на системния софтуер на управляваните от него подсистеми, да може предоставя на подсистемите обновления на информацията за нови заплахи и нови индикатори за компроментиране от глобалната система за информация на производителя или от трети източници.
REQ.206.	Решението трябва да поддържа интеграция с подсистемата (лаборатория) за динамичен анализ на зловреден код, за обмен на информация.
REQ.207.	Решението трябва да може да предоставя детайлни отчети, включително и обединена информация от управляваните подсистеми от решението.
REQ.208.	Решението трябва да може да управлява генерираните аларми от управляваните подсистеми и да може да изпраща известия, таблици и графики с данните от тях.
REQ.209.	Решението трябва да предоставя единна конзола, от която да може да се извършва централизирано конфигуриране на управляваните подсистеми, задаване на политики за сигурност, обновяване на информацията за заплахите / индикаторите за компроментиране, обновяване на системния софтуер на подсистемите.
REQ.210.	Решението трябва да позволява обновяване на управляваните подсистеми и информацията за нови заплахи дори в offline режим, без да е необходима свързаност с Интернет.

REQ.211.	Решението трябва да предоставя интегрирана централизирана администрация, в реално време, използвайки графичен интерфейс, който да предоставя следните функции: • Преглед и филтриране на събития свързани със сигурността; • Идентифициране на заразени устройства; • Централизиране на всички известия и аларми от управляваните подсистеми; • Персонализиране на графичното изобразяване на информацията (персонализиране на dashboards); • Създаване и извличане на отчети в PDF и HTML формати.
REQ.212.	Решението трябва да позволява използването и дистрибутирането на индикатори за компроментиране от трети източници (индикатори, които могат да бъдат URL адреси, IP адреси, домейни и хеш суми на зловредни файлове) към управляваните подсистеми. Индикаторите за компроментиране трябва да могат да се управляват или чрез използването на списъци за всяка категория или чрез използването на STIX (Structured Threat Information Expression) формат.
REQ.213.	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите, както и чрез Активна Директория или решения за двуфакторна автентикация.
REQ.214.	Решението трябва да може да създава, съхранява и предоставя log файлове към трети решения, използвайки Syslog протокол, например за предоставяне на информация на решения от тип SIEM.
Хардуерни изисквания – 1 брой	
REQ.215.	Устройството да е с максимална големина 2RU
REQ.216.	Устройството да разполага с поне 4TB за съхранение на данни
REQ.217.	Устройството да разполага минимално със следните портове за свързване с мрежата: 2x 1GigE BaseT
REQ.218.	Допълнителни портове: 2x 1GigE BaseT портове за управление, сериен порт, 2x Type A USB, IPMI, VGA
REQ.219.	Резервирано захранване – 1+1
REQ.220.	Устройството да може да управлява другите устройства за защита на крайни точки, за мрежова защита и за email защита, като всички те трябва да бъдат от един производител
Гаранция и поддръжка:	
REQ.221.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.222.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.223.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.224.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

5. **Подсистема за централизирано разтоварване на процесите по извършване на динамичен анализ на зловреден код и на кибератаки от другите подсистеми за киберсигурност**

Общи изисквания

REQ.225.	Решението трябва да поддържа наблюдение чрез SNMP v3.
REQ.226.	Решението трябва да може да инициализира и използва до 192 виртуални машини едновременно за sandbox анализ, за да може да обработи голям обем от трафик.
REQ.227.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.
REQ.228.	Решението трябва да може да получава автоматично данни за заплахи от засечени такива при други клиенти на вендора от цял свят.
REQ.229.	Решението трябва да може да прави анализ на големи файлове до 1024 MB.
REQ.230.	Решението трябва да може да създава локални дефиниции (signatures) на засечените зловредни файлове. Администраторите трябва да могат да конфигурират времето на изтичане на валидността на локалните дефиниции.
REQ.231.	Решението трябва да позволява модифициране на параметрите на Outlook акаунта, използван в sandbox средата.
REQ.232.	Решението трябва да може да засича webshell скриптове.
REQ.233.	Решението трябва да може да изпълнява файлове създадени от MS Office документи в startup директорията на операционната система по време на sandbox анализа.
REQ.234.	Решението трябва да може да изпълнява планираните (scheduled) задачи от зловредния код в sandbox средата.
REQ.235.	Решението трябва да позволява на администраторите да конфигурират датата и часа (времевата зона) и използвания език в sandbox средата.
REQ.236.	Решението трябва да може да извлича URL адреси от паметта по време на sandbox анализа.
REQ.237.	Решението трябва да може да извлича URL адреси от Microsoft Office файлове и от XPS файлове.
REQ.238.	Решението трябва да може да извлича и анализира свързани Relationship URL адреси.
REQ.239.	Решението трябва да може да засича зловредни Microsoft Office файлове с вградено видео в тях.
REQ.240.	Решението трябва да може да извършва анализ на следните специални файлови типове: REG, Microsoft Access, One Note, HTA и Scriptlet.
REQ.241.	Решението трябва да може да анализира Microsoft Office файлове, които са защитени с парола.
REQ.242.	Решението трябва да може да засича инжектиране на код.
REQ.243.	Решението трябва да може да извършва анализ на файлове използвайки различни версии на Microsoft Office на виртуалните машини за sandbox анализ.
REQ.244.	Решението трябва да може да извлича и анализира вградени файлове в Microsoft Office файлове.
REQ.245.	Решението трябва да може да наблюдава PowerShell дейностите в sandbox средата и да може да докладва за тях.
REQ.246.	Решението трябва да може да извлича файлове, създадени от PowerShell процеси.

REQ.247.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques) от зловредните процеси, като например PING проверки, проверки за време и техники с диалогови прозорци.
REQ.248.	Решението трябва да може да засича нови криптовируси (ransomware) в sandbox средата – без да има дефиниции (signatures) за тях.
REQ.249.	Решението трябва да поддържа Microsoft Windows 10 за засичане на drive-by атаки.
REQ.250.	Решението трябва да може да засича Point of Sale зловредни процеси.
REQ.251.	Решението трябва да може да засича зловредни процеси, използващи kernel уязвимости.
REQ.252.	Решението трябва да може да засича DDE атаки.
Хардуерни изисквания – 2 броя	
REQ.253.	Необходими са 2 броя устройства, които да могат да поемат процесите по анализиране на зловреден код, като по тази начин да може да се увеличи производителността и капацитета на работа на подсистемата за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво, както и да могат да поемат процесите по анализиране при необходимост от подсистемата за динамичен анализ на зловреден код и защита от кибератаки за мрежови файлови дялове, както и от подсистемата за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения, да може да увеличава тяхната производителност и капацитет на работа.
REQ.254.	Устройството да е с максимална големина 2RU
REQ.255.	Устройството да разполага с поне 4TB за съхранение на данни
REQ.256.	Устройството да разполага минимално със следните портове за свързване с мрежата: 1x 10/100/1000 Mbps BASE-T, 2x 10 Gbps BASE-T, 4x 10GigE SFP+
REQ.257.	Допълнителни портове: 1x 10/100/1000 Mbps BASE-T порт за управление, сериен порт, 2x Type A USB, IPMI, VGA
REQ.258.	Резервирано захранване – 1+1
REQ.259.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция и поддръжка:	
REQ.260.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.261.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.262.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.263.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

6. **Подсистема (лаборатория) за динамичен анализ на зловреден код**

Общи изисквания	
REQ.264.	Тип решение: 1 брой хардуер с вграден софтуер и 5-годишна поддръжка, 5-годишен абонамент за прилежащи услуги
REQ.265.	Решението трябва да предоставя на анализаторите на сигурността защитена среда, в която те да могат да тестват, стартират и документират процесите на сложни зловредни кодове

	(malware), като да се предоставят голям набор от виртуални машини, с предварително инсталирани операционни системи и софтуер, бивайки Windows OS (включително XP, 7, 10), Mac OSX и Linux Cent OS, като да могат да се стартират и използват поне 30 виртуални машини едновременно.
REQ.266.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.
REQ.267.	Виртуалните машини, които ще се използват за анализа, трябва да имат инсталирани най-базовите браузъри (минимално Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome, Safari), плъгини (минимално Adobe Flash) и други необходими приложения от трети разработчици (минимално Adobe Reader , VLC, QuickTime, Real Player, Microsoft Office Word, Excel, Powerpoint, Preview).
REQ.268.	Лицензите за операционните системи и за комерсиалните приложения на предварително създадените и конфигурирани виртуални машини трябва да бъдат предоставени от вендора на решението за динамичен анализ.
REQ.269.	Решението трябва да позволява автоматичното възстановяване на виртуалните машини за анализ към предварително конфигурираното им базово състояние, веднага щом приключи анализа на подадена проба от зловреден код.
REQ.270.	Решението трябва да позволява взаимодействие от анализаторите с виртуалните машини по време на динамичния анализ.
REQ.271.	Решението трябва да може да извършва анализ на поне следните файлови типове: 7zip, zip, rar, gz, 3gp, accdb, app, apk, applet, asf, asp, aspx, avi, bat, cdf, chm, cmd, com, csv , dll, dmg, doc, docx, eeml, elf, eml, exe, flv, gen, gif, hlp, hta, htm, ico, inf, inf64, jar, jpeg, jpg, js, jsp, lnk, mach-o , midi, mov, mp3, mp4, mpg, mpkg, msg, msi, one, onepkg, pdf, php, pkg, pl, png, ppsx, ppt, pptx, ps1, pub, py, pyc, qt, raw32, raw64 , rb, reg, rm, rmi, rtf, sct, sh, swf, swf built-in swf, tiff, url, url-applet, vbs, vcf, vcs, war, wav, wma, wsf, xdp, xls, xlsx, xml, xsl, shell скриптове ако са уеб-базирани (Python, Perl, Ruby), txt.
REQ.272.	Решението трябва да може да прави анализ на големи файлове до 1024 MB.
REQ.273.	Решението трябва да може да извършва статичен и динамичен анализ по поне следните методи: YARA, сканиране с антивирусни дефиниции, Python-базиран статичен анализ, засичане на dropper процеси, анализ на URL адреси, които са вградени във файлове и електронни съобщения, анализ на riskware, анализ на динамичните процеси във виртуалните машини.
REQ.274.	Решението трябва да може да анализира целия жизнен цикъл на дадена кибератака, започвайки от първоначалното проникване в системата (exploit), свързвания с хакерски команден център и сваляне на вторични зловредни модули.
REQ.275.	Решението трябва да позволява сравнението на поведението на анализирания зловреден код под различните конфигурации на средата за анализ (при различни версии на Microsoft Windows и Mac OSX операционни системи, различни версии на инсталираните приложения, различни настройки на операционните системи, при различни приложени обновления на операционните системи, при приложени различни кръпки и Service Pack версии).

REQ.276.	Предложеното решение трябва да дава възможно най-малко грешни показания и да вдига възможно най-малко грешни аларми при засичането на файлове, които наподобяват зловреден код: да алармира за поведение, което опитва да избегне засичане от системите за сигурност, инсталиране на нежелани програми, промяна на системните настройки, което влошава производителността на системите, наличие на потенциално нежелани програми (PUP) и на потенциално нежелани приложения (PUA), adware процеси и използване на инструменти, които често се използват от атакуващи хакери.
REQ.277.	Решението трябва да позволява едновременното използване на няколко виртуални машини за анализ, където различни зловредни приложения да могат да бъдат анализирани по едно и също време, без да взаимодействат помежду си.
REQ.278.	Решението трябва да може да симулира човешки действия по виртуалните машини за анализ, така че дори зловредните приложения, които имат проверки в себе си дали в момента взаимодействат с реален потребител (извиквайки някои вградени функции на Windows или от Windows API интерфейса), да се изпълнят напълно и да могат да бъдат анализирани.
REQ.279.	По време на извършване на анализа във виртуалните машини, решението трябва да може да се справя с опити от зловредния код за избягване на засичане, като например използване на ping командите, проверка на домейна, проверка на отметките в браузърите, проверка на Outlook акаунтите, проверка на активните процеси, верифициране DNS.
REQ.280.	Решението трябва да може автоматично да взаимодейства със зловредни приложения, които използват графичен интерфейс и които изискват взаимодействие с извикани диалогови прозорци или с извършване на стъпки по инсталирането на приложения.
REQ.281.	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, наскоро достъпени файлове, DNS записи.
REQ.282.	Решението трябва да позволява създаването на подробни технически отчети, които да съдържат информация за анализираните файлове, като например: • Типа на анализирания файл; • Контролните суми (MD5, SHA) на анализираните файлове / създадените файлове на виртуалните машини за анализ; • Проверка с YARA правила; • Инстинкия тип на анализирания файл; • MD5 и SHA1 стойности на първоначалния обект, но също и на всеки друг обект създаден от него; • Използваните DLL библиотеки, респективно функциите използвани от зловредния код, излвечени от IAT таблицата; • Датата на компилиране на файла; • Направените промени на ниво инсталираните приложения на системите за анализ; • Промени по файловата система; • Направените промени по Windows Registry базата от данни;

	• Извиканите Windows API функции, в хронологичен ред; • Информация за създадените / модифицираните / спрените процеси; • Информация за създадените / модифицираните / спрените Windows услуги (services); • Създадените Mutex обекти; • За всички създадени SSDT, IDT, IRP Hooks; • Направени мрежови свързвания и използвани транспортни мрежови протоколи; • Уловен мрежови трафик (под формата на PCAP файл), произтичащ от системата за анализ; • DNS заявки; • Достъпени IP адреси и използвани логически портове; • Уловени съмнителни процеси на виртуалната машина при анализа; • Записани screenshots / видео, направени по време на анализа на зловредните приложения; • Типа на използваните уязвимости (exploits) от зловредния код.
REQ.283.	Решението трябва да може да издава отчети в следните формати: PDF, CSV, Text, JSON, XML.
REQ.284.	Решението трябва да използва специално заделен мрежови интерфейс когато е пуснато в „жив“ режим, за да се избегне допускането на зловреден мрежови трафик към реалната вътрешна мрежа на организацията; Мрежовият интерфейс трябва да позволява на зловредния код да достъпва външни хакерски командни сървъри и да сваля всички допълнителни модули и артефакти, които са му необходими, за да се изпълни изцяло за анализ, включително когато мрежата е конфигурирана да използва уеб прокси.
REQ.285.	Решението не трябва да позволява мрежови комуникации от виртуалните системи/sandbox за анализ към Интернет, когато решението е пуснато в Sandbox режим: зловредния код във виртуалните машини не трябва да може да комуникира с хакерски командни центрове или URL адреси в Интернет в този режим.
REQ.286.	Решението трябва да може да засича когато зловредния код извиква sleep функции и да поставя времева точка в бъдещето, която да отговори на условието за изпълнение. Да може да симулира човешки действия като например кликване с мишката, за да може да стартира такъв тип зловреден код, използващ такива критерии.
REQ.287.	Решението да позволява на администраторите да могат да избират с кои приложения да се стартира анализа в дадена виртуалната машина.
REQ.288.	Решението трябва да може да разпознава зловредно поведение от общ характер, както и да класифицира зловредните приложения от дадено семейство вируси (троянски кон, keylogger, rootkit, RAT и т.н.) по наблюдавания модел на поведение.
REQ.289.	Решението трябва да може да използва YARA правила за разпознаване на зловреден код.
REQ.290.	Решението трябва да може да се свързва с файлови сървъри, използвайки протоколите Server Message Block или Internet File System, за анализ на съхранени файлове.

REQ.291.	Решението трябва да позволява конфигурирането на различни споделени файлови директории, в зависимост от операционната система, която ще се използва за извършването на анализ на зловреден код.
REQ.292.	Решението трябва да може автоматично да разпределя анализираните файлове към различни локации, използвайки споделени мрежови дялове, според това дали имат зловредно поведение или нямат зловредно поведение.
REQ.293.	Решението трябва да може да изпраща автоматични известия чрез Syslog, HTTP, SNMP и SMTP протоколи.
REQ.294.	Решението трябва да позволява избирането на времевия интервал, през който да бъдат проверявани споделените дялове за нови файлове.
REQ.295.	Решението трябва да може да използва прокси с автентикация за достъпване на сървъра му за обновления.
REQ.296.	Решението трябва да работи с уеб-базирана конзола за управление, която да не изисква инсталирането на допълнителен софтуер за достъпването ѝ.
REQ.297.	Решението трябва да позволява конфигурирането на ACL списък, за да се ограничат позволените свързвания с интерфейса за управление.
REQ.298.	Решението трябва да използва криптиран канал за комуникация между администраторите и конзолата за управление. Също така, трябва да позволява вмъкването на собствени дигитални сертификати на организацията, използвани за криптиране на връзката.
REQ.299.	Решението трябва да позволява локално задаване на дата и час или чрез синхронизация с NTP сървър.
REQ.300.	Решението трябва да позволява създаването на акаунти с различни роли и права, например администратори и потребители, които само следят за аларми.
REQ.301.	Решението трябва да позволява автентикиране към конзолата за управление чрез RADIUS, TACACS + и LDAP.
REQ.302.	Решението трябва да може автоматично да изпраща известия и периодично създадени отчети за „здравето“ си, използвайки SMTP.
REQ.303.	Решението трябва да позволява извличането на аларми и отчети за активността на зловреден код под формата на PDF.
REQ.304.	Решението трябва да позволява конфигурирането на съобщение, което да се показва при вписване в конзолата за управление.
REQ.305.	Решението трябва да може да се интегрира със специализирано оборудване за централизирано управление, което да може да корелира резултатите от анализите и да разпространява индикаторите за компроментиране до другите подсистеми за анализ на зловреден код.
REQ.306.	Решението трябва да може да се интегрира с Endpoint Detection and Response системи, като да може да получава артефакти от зловреден код уловен от софтуерните агенти на такъв тип система, инсталирани на ниво крайна точка или сървър.
REQ.307.	Решението трябва да може лесно да се интегрира с други подсистеми за мрежова защита и за email защита, за да се предостави информация в реално време за зловредни мрежови заявки

	(callbacks) и за споделяне на локално генерираните индикатори за компроментиране от анализите.
Хардуерни изисквания – 2 броя	
REQ.308.	Устройството да е с максимална големина 1RU
REQ.309.	Устройството да разполага с поне 4TB за съхранение на данни
REQ.310.	Устройството да разполага минимално със следните портове за свързване с мрежата: 2x 10/100/1000BASE-T Ports
REQ.311.	Допълнителни портове: сериен порт, 4x Type A USB, IPMI, VGA
REQ.312.	Резервирано захранване – 1+1
REQ.313.	Устройството да може да извършва минимално 8200 анализа на ден.
REQ.314.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция и поддръжка:	
REQ.315.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.316.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.317.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.318.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

7. **Подсистема за динамичен анализ на зловреден код и защита от кибератаки за мрежови файлови дялове (лаборатория) за динамичен анализ на зловреден код**

Общи изисквания	
REQ.319.	Тип решение: 1 брой хардуер с вграден софтуер и 5-годишна поддръжка, 5-годишен абонамент за прилежащи услуги
REQ.320.	Решението трябва да може да анализира файлове, използвайки sandbox технология, която да може да засича непознат „zero-day” зловреден код, вграден във файловете.
REQ.321.	Решението трябва да може да получава автоматично данни за заплахи от засечени такива при други клиенти на вендора от цял свят.
REQ.322.	Решението трябва да може да извършва рекурсивни автоматични сканирания, сканирания по времеви график и сканирания по ръчна заявка от администратор, за всички достъпни мрежови файлови дялове, за да да може да идентифицира и сложи под карантина всички засечени вируси по съхранените файлове, без да има значително влияние върху производителността на системите.
REQ.323.	Решението да позволява задаването на различни настройки за всяко сканиране, като да могат да се задават различни файлови типове или конкретни файлове да могат да бъдат сложени в „бял списък“, за да са изключени от сканирането.
REQ.324.	Решението трябва да позволява паузиране и продължаване на сканирания, които се извършват в даден момент (в реално време).
REQ.325.	Решението трябва да може да премества безопасните файлове в определени локации, а заразените файлове да може да премества в отделена карантина.

REQ.326.	Решението трябва да може да връща файлове в първоначалните им локации, след като са освободени от карантината.
REQ.327.	Решението трябва да може да издава пълни отчети за поведението на файловете – прилежащи процеси, достъп до файловете/записани файлове на дисковото пространство, промени в регистрите на операционната система.
REQ.328.	Решението трябва да може да споделя откритите от него индикатори за компроментиране с останалите подсистеми, за динамичен анализ на зловреден код и за разследвания за кибератаки, също така да може и да получава индикатори за компроментиране от тях.
REQ.329.	Решението трябва да предоставя настройки на филтри при сканирането на файлове, според типа на файловете, локацията им, последната дата на модифициране.
REQ.330.	Решението трябва да позволява използването на YARA правила, версия 3.4.
REQ.331.	Решението трябва да може да извършва освен динамичен анализ, така и статичен анализ. Администраторите трябва да могат да избират дали да се извършва статичния анализ.
REQ.332.	Решението трябва да може да анализира файлове с големина до поне 1024 MB. Максималният размер на файловете, които ще се анализират, да може да бъде променян.
REQ.333.	Решението трябва да може да прави морфологичен разбор на .eml файлове.
REQ.334.	Решението трябва да може да извлича прикачени файлове от .eml файлове. Броя на прикачени файлове, които да се анализират, трябва да може да бъде променян.
REQ.335.	Решението трябва да може да създава локални дефиниции (signatures) на засечените зловредни файлове след динамичен анализ. Администраторите трябва да могат да конфигурират времето на изтичане на валидността на локалните дефиниции.
REQ.336.	Решението трябва да може да се интегрира по подразбиране с Microsoft Office 365 за обработка на файлове.
REQ.337.	Решението трябва да може да се интегрира по подразбиране с Microsoft OneDrive за обработка на файлове. Решението трябва да може да извършва динамичен анализ на файловете в облачното пространство на OneDrive.
REQ.338.	Решението трябва да може да се интегрира по подразбиране с Microsoft SharePoint Online, за защитено споделяне на файлове.
REQ.339.	Решението трябва да може да изпраща известия за събития по email, HTTP, Rsyslog, SNMP в XML, JSON или в текстов формат.
REQ.340.	Решението трябва да поддържа следните протоколи: CIFS, NFS, WebDAV, Secure WebDAV.
REQ.341.	Решението трябва да позволява избирането на кои файлови хранилища да се сканират, директно от графичния интерфейс за управление.
REQ.342.	Решението трябва да може да извлича първоначална информация за споделените дискови пространства, като например брой и тип на файловете на тях, за да може по-лесно да се определят критериите за сканирането им от решението.
REQ.343.	Решението трябва да предоставя информация за резултатите след извършване на сканиране.
REQ.344.	Решението трябва да може да предоставя детайлни отчети във формати .xml, .json, .csf и текстов формат, както и обобщителни отчети в .pdf формат.

REQ.345.	Решението трябва да позволява определянето на времеви график за автоматично изготвяне и изпращане на отчети.
REQ.346.	Решението трябва да позволява лесно извличане на резултати от анализи в PDF формат.
REQ.347.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление.
REQ.348.	Решението трябва да може да се интегрира с подистемата за централизирано управление и да може да се конфигурира от нея. Трябва да могат да се получават системни обновления през подсистемата за централизирано управление и да се обменят аларми и известия.
REQ.349.	Решението трябва да може да анализира файловете в локален sandbox, както и да може да изпраща файловете за анализ към външен sandbox, когато устройството е претоварено.
REQ.350.	Решението трябва да разполага с IPMI интерфейс.
REQ.351.	Решението трябва да поддържа AAA протокол за контрол на потребителския достъп.
REQ.352.	Решението трябва да разполага с вградени функции за филтриране на IP адреси, за да се защити интерфейса за управление от нежелан достъп.
REQ.353.	Решението трябва да позволява определянето на използваните ресурси за sandbox анализ, за да се избегне претоварване на системата.
REQ.354.	Решението трябва да поддържа наблюдение на показатели чрез SNMP.
REQ.355.	Решението трябва да предоставя функции за защитено изтриване на съхранени данни.
REQ.356.	Решението трябва да може да използва поне 190 виртуални машини за sandbox анализ по едно и също време.
REQ.357.	Решението трябва да може да извършва автоматичен анализ на поне 60000 потенциално зловредни обекта на ден.
REQ.358.	Решението трябва да може да докладва за опитите за мрежово свързване на анализираните обекти във виртуалните машини.
REQ.359.	Решението да може да извършва следствен анализ на откритите зловредни файлове и да може да предоставя копие на бинарния им (двоичен) код, както и PCAP файл с опитите им за мрежови свързвания, заедно с всички посетени URL адреси.
REQ.360.	Решението трябва да може да извършва динамичен анализ за зловреден код, да може да се обновява и да може да му се предоставя нова информация за заплахи, дори в offline режим, без да има връзка с Интернет.
REQ.361.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.
REQ.362.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques).
REQ.363.	Решението трябва да разполага с графичен интерфейс, където да се изобразяват пълните детайли от извършения анализ на зловреден код.
REQ.364.	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, използван Outlook акаунт, използвани език и часова зона.

REQ.365.	Решението трябва да може да тества и засича зловреден код в различни операционни системи на виртуалните машини за sandbox анализ, с различни версии на service pack, като да се поддържат както x64, така и x86 архитектури, под Windows и под Mac.
REQ.366.	Решението трябва да може да извършва детайлен анализ и да открива зловреден код в следните файлови формати (минимално): изпълними .exe файлове, JAVA, PDF, MS Office документи, често срещани мултимедийни файлови формати като JPEG, QuickTime, MP3, архиви тип ZIP/RAR/7ZIP/TNEF, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm.
REQ.367.	Решението трябва да позволява на администраторите да посочат кои приложения във виртуалните машини за анализ да стартират кои файлови типове.
REQ.368.	Решението трябва да може да извършва цялостен анализ локално, без да е необходимо да излиза информация извън структурите на организацията.
REQ.369.	Решението трябва да поддържа LDAP или RADIUS методи за вписване на потребителите (минимално).
REQ.370.	Решението трябва да разполага с команден и с графичен интерфейс (достъпен през стандартен уеб-браузър) за централизирано управление.
REQ.371.	Решението трябва да може да работи в следните режими (за анализиране на файлове): • Сканиране по ръчни заявки (on-demand, с възможност и за анализ на отделни файлове) • Продължително сканиране на посочени файлови хранилища.
REQ.372.	Решението трябва да позволява избирането на различни локации за преместване на файлове след анализ според това дали са със статус на „добър“, „неизвестен“ или „лош“.
Хардуерни изисквания – 1 брой	
REQ.373.	Устройството да е с максимална големина 2RU
REQ.374.	Устройството да разполага с поне 2TB за съхранение на данни
REQ.375.	Устройството да разполага минимално със следните портове за свързване с мрежата: 4x 1GigE BaseT
REQ.376.	Допълнителни портове: сериен порт, 4x Type A USB, IPMI
REQ.377.	Резервирано захранване – 1+1
REQ.378.	Устройството да може да анализира минимално 60000 файла на ден.
REQ.379.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция и поддръжка:	
REQ.380.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.381.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.382.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.383.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

8. **Подсистема за улавяне на мрежови пакети, разследвания и централизиран анализ и визуализация**

Общи изисквания	
REQ.384.	Тип решение: • 1 брой хардуер за улавяне на мрежови пакети, с вграден софтуер и 5-годишна поддръжка; • 1 брой хардуер за разследвания и централизиран анализ и визуализация, с вграден софтуер и 5-годишна поддръжка;
REQ.385.	Решението трябва да има пълна видимост над мрежовия трафик, чрез високоскоростно улавяне на мрежови пакети и анализ при мрежова производителност от 1800 Mbps за 4 интерфейса на ниво gateway. Решението трябва да може да се поставя в TAP/SPAN режим на работа, като да може да получава мрежовите данни след SSL декриптиране от настоящо решение за SSL декриптиране на организацията от трети производител (да има възможност за интеграция).
REQ.386.	Решението да има възможност за изключително бързо (в реално време) записване и индексиране на мрежови трафик.
REQ.387.	Решението трябва да може да улавя, търси и анализира информацията от мрежовите пакети и сесии.
REQ.388.	Решението трябва да може да чете и записва пакети в PCAP формат.
REQ.389.	Решението трябва да позволява извършването на филтрирани търсения, използвайки често срещани стойности за адрес, приложение, протокол, VLAN, MPLS, метаданни от мрежовата връзка.
REQ.390.	Решението трябва да поддържа интеграция с подсистема за засичане, защита и разследнване на непознати заплахи на ниво крайна точка, за да може да получава информация за вътрешно наблюдаваните IP адреси от крайните точки и за да може да извлича потребителските имена, асоциирани с дадено име на хост.
REQ.391.	Решението трябва да може да анализира мрежови сесии и да извлича файлове от тях.
REQ.392.	Решението трябва да позволява на анализаторите да търсят в мрежовия трафик ключови думи и регулярни изрази на ниво приложен слой.
REQ.393.	Решението трябва да поддържа сложни заявки, използващи булева логика.
REQ.394.	Решението трябва да може да се интегрира и изпраща извлечени файлове от мрежови сесии директно към подсистема (лаборатория) за динамичен анализ на зловреден код.
REQ.395.	Решението трябва да може да реконструира уеб-страници и email съобщения от уловения мрежови трафик. Също така, трябва да може да реконструира POP3/IMAP/FTP/SMB.
REQ.396.	Решението трябва да може да извлича данни от много големи файлове с мрежови трафик, до 1 гигабайт.
REQ.397.	Решението трябва да може да кодира/декодира следните формати от данни: Base64, gzip, HEX, HEXDUMP, JSON, URL, XOR.
REQ.398.	Решението трябва да позволява определянето на собствени правила, на базата на които да се улавя и съхранява мрежовия трафик за по-нататъшен анализ.

REQ.399.	Решението трябва да може да анализира в детайли следните протоколи: DCE-RPC, IPv6, SMB, DHCP, IRC, SMB2, DNS, MODBUS, SMTP, ERSPAN, MPLS, SSL, FTP, MSN, SSH, GRE, POP3, TCP, HTTP, PPP, TEREDO, ICMPv4, RDP, TLS, ICMPv6, RTSP, UDP, IMAP, SCTP, VLAN, IPv4, SIP, IPFIX, NETFLOWv5, NETFLOWv9.
REQ.400.	Решението трябва да позволява търсене в индексираните метаданни на следните протоколи: HTTP, DNS, SMTP, POP3, IMAP, SSL, TLS, FTP, SSH и MODBUS.
REQ.401.	Решението трябва да може да разпознава минимално следните приложения: AFP, Aimini, Amazon, Apple, AppleiCloud, AppleiTunes, AppleJuice, Armagetron, AVI, Ayiya, BattleField, BGP, BitTorrent, CiscoSkinny, CiscoVPN, Citrix, Citrix_Online, CNN, Collectd, Corba, Crossfire, DCE_RPC, DHCP, DHCPV6, DirectConnect, Direct_Download_Link, DNS, Dofus, DropBox, eBay, eDonkey, EGP, EPP, Facebook, FacebookChat, FastTrack, Fiesta, Filetopia, Flash, Florensia, FTP, FTP_CONTROL, FTP_DATA, GMail, Gnutella, Google, GoogleMaps, GRE, GrooveShark, GTP, Guildwars, H323, HalfLife2, HTTP, HTTP_Application_ActiveSync, HTTP_APPLICATION_VEOHTV, HTTP_Connect, HTTP_Proxy, IAX, IceCast, ICMP, ICMPV6, IGMP, IMAP, IMAPS, iMESH, IPP, IPsec, IP_in_IP, IRC, Jabber, Kerberos, Kontiki, LastFM, LDAP, LLMNR, LotusNotes, MapleStory, MDNS, Meebo, Megaco, MGCP, MMS, Move, MPEG, MSN, MsSQL, MySQL, NetBIOS, NetFlix, NFS, NOE, NTP, OggVorbis, OpenFT, OpenVPN, Oracle, Oscar, OSPF, Pandora, Pando_Media_Booster, PcAnywhere, POP, POP3, POPS, PostgreSQL, PPLive, PPStream, PPTP, QQ, QQLive, Quake, QuickTime, Radius, RDP, RealMedia, Redis, RemoteScan, RSYNC, RTCP, RTMP, RTP, RTSP, SAP, SCTP, sFlow, ShoutCast, SIP, SkyFile_PostPaid, SkyFile_PrePaid, SkyFile_Rudics, Skype, SMB, SMTP, SMTPS, SNMP, SOCKS4, SOCKS5, Socrates, Sopcast, Soulseek, Spotify, SSDP, SSH, SSL, SSL_No_Cert, Stealthnet, Steam, STUN, Syslog, TDS, TeamSpeak, TeamViewer, Telegram, Telnet, TFTP, Thunder, TOR, TruPhone, Tuenti, Tvants, TVUplayer, Twitter, UbuntuONE, Unencryped_Jabber, Unknown, UPnP, Usenet, VEOHTV, VHUA, Viber, VMware, VNC, VRRP, Warcraft3, Webex, WebM, Whois-DAS, WhatsApp, Wikipedia, WindowsMedia, WindowsUpdate, WinMX, WorldOfKungFu,WorldOfWarcraft, Xbox, XDMCP, Yahoo, YouTube, Zattoo, ZeroMQ.
REQ.402.	Решението трябва да може да анализира следните видове мрежови трафик: използващ IPv4 протокол; използващ IPv6 протокол.
REQ.403.	Решението трябва да предоставя на администраторите разбираем и с възможност за модифициране интерфейс със списъци, графики и географски карти.
REQ.404.	Решението трябва да позволява на администраторите лесно и бързо да извършват „reverse DNS lookup“ и „whois“ проверки директно от уеб интерфейса.
REQ.405.	Решението трябва да позволява на анализаторите да преглеждат данните на ниво мрежова връзка, пакет и payload.
REQ.406.	Решението трябва да може да приема аларми от другите подсистеми за киберсигурност.
REQ.407.	Решението за улавяне на мрежови пакети трябва да използва „full disk encryption“ метод за криптиране на събраните данни и метаданни.
REQ.408.	Решението за улавяне на мрежови пакети трябва да може да се интегрира с SAS RAID или с HBA контролер, за да се гарантира непрекъснат процес на събирането на мрежови пакети.
REQ.409.	Решението трябва да разполага с IPMI интерфейс.

REQ.410.	Решението трябва да поддържа автентикация на потребителите с протоколи PAM/LDAP/RADIUS/TACACS+. Да се поддържа ролево-базирано управление, потребителите да могат да имат различни роли (администратор, анализатор, т.н.)
REQ.411.	Решението трябва да може да засича извличане на данни извън организацията.
REQ.412.	Решението трябва да поддържа Suricata правила за дефиниции/алармиране.
REQ.413.	Решението трябва да позволява задаването на правила за филтриране на мрежовия трафик. Правилата са необходими за намаляване на обема анализиран трафик. Тези правила трябва да са наложени директно на хардуерните интерфейси за улавяне на трафика, преди да затормозят централният процесор на системата. Да може да се филтрира минимално на база следните параметри: src IP, src port, dst IP, dst port.
REQ.414.	Решението трябва да може да извлича метаданни от уловения мрежови трафик през HTTP.
REQ.415.	Решението трябва да може да индексира в реално време уловените мрежови пакети, използвайки маркери за време и атрибутите на мрежовите свързвания. Да могат да се извличат индекса на потока от данни и метаданните на мрежовата връзка в JSON формат.
REQ.416.	Решението трябва да предоставя информация за собствените си процеси и за складираните данни, за да може да се планира капацитета в бъдеще.
REQ.417.	Решението трябва да позволява да му се наблюдават параметрите по производителността чрез SNMP.
REQ.418.	Решението трябва да предоставя възможност за сигурно изтриване на данните от дисковото му пространство, чрез презаписване (overwrite) на данните множество пъти.
REQ.419.	Решението трябва да може да се интегрира с източници на информация за заплахи.
REQ.420.	Решението трябва да позволява добавянето на множество нови индикатори за компроментиране чрез формати STIX и OpenIOC.
REQ.421.	Решението трябва да позволява определяне на времеви интервал за автоматично търсене за индикатори за компроментиране в събраните метаданни и да може да вдига аларми за тях.
REQ.422.	Решението трябва да поддържа изпозлването на reverse SSH и HTTPS тунели, за да може да се интегрира със системи от външна мрежа.
REQ.423.	Решението трябва да поддържа автентикация с използване на smart карти.
REQ.424.	Решението трябва да предоставя достъп за търсене в съхранените метаданни.
REQ.425.	Решението трябва да може да се интегрира и да приема метаданни на слой 7 от подсистема за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво, както и да може да изисква уловени пакети по конкретно събитие, за което е вдигната аларма.
REQ.426.	Решението трябва да разполага с API интерфейс.
REQ.427.	Решението за улавяне на мрежови пакети трябва да е изградено с подсилена откъм сигурност, заключена операционна система.
REQ.428.	Решението за улавяне на мрежови пакети трябва да може да съхранява събраните PCAP данни и метаданни за поне 14 дена, при събиране на данни 8 часа на ден при количество трафик от 1 Gbps.
Хардуерни изисквания за хардуерно устройство за улавяне на мрежови пакети	
REQ.429.	Устройството да е с максимална големина 2U

REQ.430.	Устройството да разполага с поне 95TB за съхранение на данни, с възможност за разширяване на обема със скачено SAS дисково пространство
REQ.431.	Устройството да разполага минимално със следните портове за свързване с мрежата: 4 x 10GE SFP+
REQ.432.	Допълнителни портове: 2 x 1GbE портове за управление
REQ.433.	Резервирано захранване – 1+1
REQ.434.	Устройството да може да записва мрежови данни със скорост от 1800 Mbps
Хардуерни изисквания за хардуерно устройство за разследвания и централизиран анализ и визуализация	
REQ.435.	Устройството да е с максимална големина 2U
REQ.436.	Устройството да разполага с поне 45TB за съхранение на данни
REQ.437.	Резервирано захранване – 1+1
Гаранция и поддръжка:	
REQ.438.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.439.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.440.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.441.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.