ИНФОРМАЦИОННО ОБСЛУЖВАНЕ
1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340,
office@is-bg.net www.is-bg.net
ЕИК: 831641791

ЗАПИТВАНЕ ЗА ОФЕРТА

„Информационно обслужване" АД, със седалище и адрес на управление: гр. София, ул. „Панайот Волов" № 2, тел. 02/9420332, e-mail: office@is-bg.net, представлявано от **Ивайло Филипов – Изпълнителен директор**, Ви кани да участвате в процедура за избор на доставчик при следните условия:

1. Предмет на процедурата:

„Придобиване на лицензи за платформа за създаване на стратегия за привличане на киберпрестъпници с цел ранно откриване на различните техники и методи на атака за период от 36 месеца за нуждите на „Информационно обслужване" АД".

2. Срокове за изпълнение:

2.1. Срок за доставка на лицензи за платформа за създаване на стратегия за привличане на киберпрестъпници с цел ранно откриване на различните техники и методи на атака за период от 36 месеца - до 10 (десет) работни дни, считано от датата на влизане в сила на договора.

2.2. Срокът на валидност и поддръжка на лицензите по т. 1 е 36 (тридесет и шест) месеца, считано от датата на приемо-предавателния протокол за доставка.

3. Списък на документите, които кандидатите следва да представят към офертата:

3.1. ОФЕРТА – изготвена по образец (Приложение № 2).

3.2. Документ/оторизация от производителя - участникът следва да бъде надлежно оторизиран от производителя на софтуера или от негов официален представител за предоставено право на извършване на разпространение на предлаганите софтуерни продукти на територията на Република България.

Участникът доказва съответствието си с поставеното изискване чрез прилагане на оторизационни писма или други еквивалентни документи, издадени от производителите или от официални техни представители на български език или придружени от превод на български език.

В случаите на представяне от участника на оторизационни писма от официални представители на производителите (или еквивалентни документи), в офертата се прилагат и оторизационни писма, издадени от производителите (или еквивалентни документи), с които се упълномощават официалните представители на производителите, на български език или придружени от превод на български език.

4. Критерии за оценка на офертите:

Всички оферти, които отговарят на изискванията съгласно Количествена и техническа спецификация - Приложение № 1, ще бъдат оценявани по критерия „най-ниска предложена цена", като се оценява предложената обща цена в лева без ДДС. На първо място ще бъде класиран кандидатът, предложил най-ниска обща цена в лева без ДДС.

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340,
office@is-bg.net www.is-bg.net
ЕИК: 831641791

5. Максимална обща цена - кандидатите следва да предложат цена, която не надвишава определената максимална обща цена в размер на 300 000.00 (триста хиляди) лева без ДДС.

Кандидат, предложил по-висока от максималната обща цена, ще бъде отстранен от участие в процедурата.

6. Изисквания към офертата:

6.1. Офертата се изготвя по образец (Приложение № 2);

6.2. Посочва се единична и обща цена в лева без ДДС, която да включва всички разходи за изпълнение на предмета на процедурата;

6.3. Начин на плащане – извършва се по банков път, в срок до 30 (тридесет) календарни дни, след подписване на приемо-предавателен протокол за приемане без възражения и забележки от Възложителя и издадена фактура от Изпълнителя;

6.4. Срок на валидност на офертата съгласно т. 7;

6.5. Срок за изпълнение – съгласно т. 2.

7. Срок на валидност на офертата – срокът на валидност да бъде не по-малко от 60 (шестдесет) календарни дни, считано от датата на представяне на офертата.

8. Лице за контакти с „Информационно обслужване" АД

Симеон Кърцелянски - ръководител отдел, „Киберзащита и управление на информационната сигурност", отдел „Киберзащита и управление на информационната сигурност", мобилен: +359 877 469 169, e-mail: s.kartselyanski@is-bg.net.

9. Подаване на офертата:

9.1. Срок, място и начин:

Офертата следва да бъде подадена по електронен път в срок **до 12:00 часа на 05.09.2025 г.**, на следния електронен адрес: office@is-bg.net.

9.2. Изисквания към представянето на офертата:

Офертата се съставя като електронен документ във формат .pdf и се подписва с квалифициран електронен подпис.

Ако към офертата е необходимо да бъде представен документ, който е издаден на хартиен носител, същият се представя сканиран и заверен с квалифициран електронен подпис.

В случай, че обстоятелства от документите за идентификация и квалификация са достъпни чрез публичен безплатен регистър или информацията е публично достъпна на друг официален адрес, кандидатите могат да посочат електронен адрес, на който тази информация е налична и достъпна.

Електронното съобщение (e-mail), с което се подава офертата за участие по настоящата процедура следва да съдържа данни за:

1. наименованието на участника;

2. телефон и електронен адрес;

3. наименованието на процедурата, за която се подават документите.

За дата и час на получаване на офертата се приемат датата и часа на получаване на офертата на посочения в т. 9.1 адрес на електронна поща за подаване на оферти.

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340,
office@is-bg.net www.is-bg.net
ЕИК: 831641791

„Информационно обслужване“ АД използва инструменти за осигуряване на сигурността на информацията, предавана по електронна поща, които могат да забавят получаването на електронни съобщения, поради което е препоръчително офертите за участие по настоящата процедура да се изпращат най-малко 30 минути преди крайния срок по т. 9.1.

10. Участници в процедурата:

В процедурата могат да участват и кандидати, до които не е изпратено изрично запитване за оферта.

Приложения:

1. Количествена и техническа спецификация (Приложение № 1);
2. Образец на ОФЕРТА (Приложение № 2).

ИВАЙЛО ФИЛИПОВ
ИЗПЪЛНИТЕЛЕН ДИРЕКТОР
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ” АД

ИНФОРМАЦИОННО ОБСЛУЖВАНЕ

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340,
office@is-bg.net www.is-bg.net
ЕИК: 831641791

Приложение № 1

Количествена и техническа спецификация

за „Придобиване на лицензи за платформа за създаване на стратегия за привличане на киберпрестъпници с цел ранно откриване на различните техники и методи на атака за период от 36 месеца за нуждите на „Информационно обслужване“ АД“

Минимални технически изисквания	
REQ. 1.	Предложената платформа трябва да включва 30 лицензи за 300 симулирани deception крайни точки (групирани по 10 в лиценз) и неограничен брой honeypot елементи. Предложените лицензи трябва да са с валидност и включена поддръжка за период от 36 месеца.
REQ. 2.	Предложената платформа трябва да може да се имплементира, без да се налага промяна в съществуващата мрежова топология на организацията.
REQ. 3.	Предложената платформа трябва да се състои минимално от следните елементи: конзола за централизирано управление, крайни точки-капани, агенти за разпространение на honeypot елементи (breadcrumbs) по крайните точки.
REQ. 4.	Предложената платформа трябва да може да се поставя във виртуална среда, като минимално да се поддържат следните хипервайзори: VMware vSphere 6.0/6.5/7.0, Microsoft Hyper-V 2016 или по-нова версия, Microsoft Azure Cloud, KVM-базирани платформи (например Proxmox, OpenStack и т.н.).
REQ. 5.	Платформата трябва да може да поставя фалшиви данни (breadcrumbs) на реални мрежови хостове от средата, като да се поддържат минимално хостове под Linux и Microsoft Windows операционни системи.
REQ. 6.	Платформата трябва да е скалируема без да се налага преинсталиране на системните му компоненти за целта.
REQ. 7.	Платформата трябва да поддържа архитектура с множество инстанции на крайните точки-капани, управлявани централизирано.
REQ. 8.	Платформата трябва да позволява поставянето на крайни точки-капани в различни мрежови сегменти, използвайки различни конфигурации според сегмента.
REQ. 9.	Палтформата трябва да може да разчита само на собствените си компоненти и да функционира изцяло, без да е необходимо да получава данни от трети източници за IP мрежови потоци (да не са му необходими сурово копие на трафика, NetFlow, sFlow, jFlow или мрежови потоци от какъвто и да е тип от други решения).
REQ. 10.	Платформата трябва да може да работи както с маркиран (tagged), така и с немаркиран (untagged) мрежови трафик.
REQ. 11.	Платформата трябва да разполага с централизирана конзола за управление, която да е достъпна през уеб-браузър, като минимално да се поддържат най-новите версии на следните браузъри: Mozilla Firefox, Safari, Google Chrome.
REQ. 12.	Платформата трябва да позволява централизирано управляване на множество изолирани подорганизации с цялостно разделение на данните им (multitenancy).
REQ. 13.	Платформата трябва да позволява създаването на администраторски акаунти с ограничени права за достъп само до даден мрежови сегмент от управляваните от платформата среди.

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340,
office@is-bg.net www.is-bg.net
ЕИК: 831641791

REQ. 14.	Платформата трябва да поддържа използването на ролево-базиран контрол на достъпа с грануларно разпределяне на права.
REQ. 15.	Платформата трябва да може да извършва и предоставя одит лог на всички действия с него в централизираната конзола за управление, като минимално да се регистрират всички промени по конфигурации, с предходна и текуща стойност.
REQ. 16.	Платформата трябва да поддържа използването на многофакторна автентикация и използването на алгоритъм за еднократни пароли.
REQ. 17.	Платформата трябва да включва вградени инструменти за сервизни услуги на компонентите ѝ, минимално с функции за ping, traceroute, htop, packet capture.
REQ. 18.	Платформата трябва да може да предоставя статуса на процесите по създаване на примамки.
REQ. 19.	Всяка от крайните точки-капани на Платформата трябва да е уникална, със собствени характеристики за MAC адрес, IP адрес, име на хоста, набор от симулирани услуги и настройки.
REQ. 20.	Крайните точки-капани на платформата не трябва да използват IP-alias-базирана скалируемост, където всяка точка да разполага с множество IP адреси, тъй като това позволява на атакуващите по-лесно да разпознаят капаните в инфраструктурата.
REQ. 21.	Крайните точки-капани трябва да разполагат минимално с автоматизирани функции за периодично: -свързване към външни мрежови ресурси -проверяване на своите имена и използвани домейни чрез DNS, mDNS, LLMNR и NetBIOS -изискват списък с файлови реурси SMB (Windows File Share) протокол.
REQ. 22.	Платформата трябва да поддържа използването на минимално следните типове фалшиви данни (breadcrumbs): -запазени данни за автоматично вписване в среди -профили за мрежови свързвания към симулирани източници на данни -линкове към мрежови ресурси -запазени RDP и SSH сесии.
REQ. 23.	Платформата трябва да може да засича опити за пробив в сигурността, минимално brute force атаки и опити за свързване със симулирани услуги с отбелязана различна степен на критичност. Функцията за засичане на пробиви трябва да може да работи както с некриптиран, така и с криптиран мрежови трафик.
REQ. 24.	Платформата трябва да може да предоставя информация за свързванията с крайните точки-капани и извършените действия върху тях, минимално: -информация за IP адреса на компроментирания хост -информация за компроментирани данни за вписване -информация за използвани протоколи и портове.
REQ. 25.	Платформата трябва да разполага с графични панели с информация за функционирането на системите, настъпили събития и т.н., с възможност за дълбаене в тях до достигане на конкретна детайлна информация.
REQ. 26.	Платформата трябва да може да засича атаки от тип man-in-the-middle, включително: -ARP spoofing -манипулиране на резултатите от NBT/LLMNR/mDNS услуги -подслушване на HTTPS заявки.
REQ. 27.	Платформата трябва да може да работи в автоматизиран режим, където да може автоматично да създава крайни точки-капани при необходимост.

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340,
office@is-bg.net www.is-bg.net
ЕИК: 831641791

REQ. 28.	Платформата трябва да разполага минимално със следните варианти за крайни точки-капани: -Microsoft Windows с RPC, WinRM, RDP услуги -Microsoft SMB файлов сървър -сървъри с Linux-базирани операционни системи -Qradar с потребителски уеб интерфейс -VMware ESX с потребителски уеб интерфейс -FortiGate с потребителски уеб интерфейс -SCADA системи: HMI/PLC/Ethernet процесор/Modbus TCP сървър -DNS сървър -бази от данни: MySQL сървър, PostgreSQL сървър -FTP файлов сървър -TFTP сървър -Samba файлов сървър -MQTT брокер -Telnet сървър -Email сървъри, минимално: Microsoft Outlook с потребителски уеб интерфейс, Zimbra Collaboration сюита, Kerio Connect пощенски сървър, Roundcube пощенски сървър, базов Exim4 MTA. -VoIP, минимално: базов Asterisk PBX, Asterisk с FreePBX графичен интефейс, 3CX телефонна система, Grandstream UCM6202 PBX.
REQ. 29.	Платформата трябва да може да създава мрежови капани, базирани на който и да е уебсайт и която и да е уеб услуга, които са използвани в организацията. Тези капани трябва да могат да засичат опити за възползване от познати уязвимости от OWASP TOP 10 модела.
REQ. 30.	Мрежовите капани трябва да имат възможност за настройване на минимално следните параметри: -хедър на сървър за симулиране на уеб услуги -Rate-лимитер за справяне с DoS атаки срещу капаните -добавяне на собствени задължителни HTTP хедъри -добавяне на TLS сертификат към мрежовия капан.
REQ. 31.	Платформата трябва да може автоматично да попълва капаните с избрани потребителски данни чрез извличане на информация от база от данни или от архиви под формата на прикачени файлове.
REQ. 32.	Платформата трябва да позволява създаването на Windows-базирани хостове с различни версии на операционната система, включително с поддръжка на по-стари версии, минимално Windows XP, Windows Server 2003, Windows 8, Windows Server 2012 Datacenter, Windows Server 2008 R2.
REQ. 33.	Платформата трябва да поддържа функция за регенериране на използвани файлови капани, както и на мрежови капани, при необходимост.
REQ. 34.	Платформата трябва да разполага с капани за OT инфраструктури, минимално за SIEMENS и Allen-Bradley от Rockwell Automation. Капаните трябва да могат да поддържат минимално S7comm и Modbus TCP протоколи.
REQ. 35.	Платформата трябва да може да корелира и класифицира сходни събития, свързани с конкретни атаки, в единна аларма.
REQ. 36.	Платформата трябва да предоставя възможност за създаване на собствени типове мрежови капани, на базата на вече съществуващите типове в системата. След създаването на собствен мрежови капан, Платформата трябва да предоставя функция за автоматично създаване на множество капани от дадения тип, без да се налага ръчна интервенция. Настройването на новите мрежови капани трябва да

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340,
office@is-bg.net www.is-bg.net
ЕИК: 831641791

	може да се извършва в опростен текстов формат (минимално да се поддържат YAML или JSON формати).
REQ. 37.	Платформата трябва да разполага с вградена IRMS (Incident Response Management System) функционалност, показваща статуса на всяка обработена аларма.
REQ. 38.	Honeypot елементите на платформата трябва да допускат ниво на интерактивност що се отнася до извършване на заявки за данни за вписване и предоставяне на графичен или текстови интерфейс за управление.
REQ. 39.	Платформата трябва да може да засича киберзаплахи, без да използва антивирусни дефиниции.
REQ. 40.	Платформата трябва да може да предоставя визуализация на взаимовръзките между мрежовите активи на организацията.
REQ. 41.	Платформата трябва да може да предоставя извадки от мрежовия трафик, свързан с дадена аларма за инцидент, минимално в PCAP формат.
REQ. 42.	Платформата трябва да позволява изграждането на бели списъци от допустими услуги, за да се гарантира ниско ниво на грешните показания. Трябва да може да се определя допустим времеви период на валидност за всяко от изключенията в списъка.
REQ. 43.	Платформата трябва да разполага с функция при избор за автоматично маркиране на генерираните аларми като игнорирани, за целите на външни тестове.
REQ. 44.	Платформата трябва да разполага с функция за тестване на мрежовата инфраструктура, поддържаща извършването на различни тестове и симулации, за целите на засичане на слаби звена от текущата инфраструктура.
REQ. 45.	Модулът за тестване на мрежовата инфраструктура трябва да може да извършва мрежови сканирания, на база на резултатите от които да предоставя набор от действия за извършване върху откритите мрежови активи.
REQ. 46.	Модулът за тестване на мрежовата инфраструктура трябва да поддържа следните мрежови услуги: DNS, FTP, SSH, SAMBA, RDP, HTTP.
REQ. 47.	Модулът за тестване на мрежовата инфраструктура трябва да е интегриран в платформата и да не изисква инсталирането на допълнителни елементи.
REQ. 48.	Модулът за тестване на мрежовата инфраструктура трябва да може да покрива минимално тактиките от фазите "Reconnaissance" и "Initial Access" на MITRE модела.
REQ. 49.	Платформата трябва да разполага с функция за интегриране на фалшифите данни-примамки и фалшивите потребителски акаунти в налична Активна директория на организацията.
REQ. 50.	Платформата трябва да поддържа автоматичното създаване на DNS записи за добавените компютърни акаунти на Платформата в Активна директория.
REQ. 51.	Платформата трябва да позволява автоматизация на добавянето на фалшиви активи в Активна директория чрез използване на скриптове от платформата, които да могат предварително да се тестват, преди да се приложат в продуктова среда.
REQ. 52.	Платформата трябва да позволява активно да се мониторират фалшивите потребителски акаунти и да може да засича Kerberoasting и AS-REP Roasting атаки с тях, както и опити за използване на фалшивите акаунти за автентикация в системи.
REQ. 53.	Платформата трябва да може да мониторира поне три домейна и при засичане на данни за вписване от тези домейни като изтекли извън организацията в dark web, Платформата трябва да може да вдига аларми за инцидента.

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340,
office@is-bg.net www.is-bg.net
ЕИК: 831641791

REQ. 54.	Платформата трябва да може да се интегрира с EDR платформи, решения за мрежова сигурност, SIEM системи.
REQ. 55.	Платформата трябва да може да се интегрира със среди за колаборация за изпращане на аларми, включително Slack и Microsoft Teams.
REQ. 56.	Платформата трябва да позволява изпращането на автоматични известия за аларми чрез email.
REQ. 57.	Платформата трябва да позволява изпращането на информация към трети SIEM системи чрез syslog през TLS комуникация.
REQ. 58.	Платформата трябва да позволява изпращането на автоматични известия за аларми чрез Webhook.
REQ. 59.	Платформата трябва да разполага с добре описан API интерфейс, с минимално следните функции: -добиване на информация за системите, включително за лицензите на платформата, управляваните среди, капани и вдигнати аларми. -управление на състоянието на крайните точки-капани и на инцидентите със сигурността.
Гаранция и поддръжка:	
REQ. 60.	Период на поддръжка: минимум 36 месеца
REQ. 61.	Тип поддръжка: 24x7x365
REQ. 62.	Възможност за обновление на софтуера в периода на поддръжката до последна актуална версия на производителя.

Изисквания към изпълнението:

1. Участникът следва да бъде надлежно оторизиран от производителя на софтуера или от негов официален представител за предоставено право на извършване на разпространение на предлаганите софтуерни продукти на територията на Република България.

Участникът доказва съответствието си с поставеното изискване чрез прилагане на оторизационни писма или други еквивалентни документи, издадени от производителите или от официални техни представители на български език или придружени от превод на български език в Техническото си предложение.

В случаите на представяне от Участника на оторизационни писма от официални представители на производителите (или еквивалентни документи), в офертата се прилагат и оторизационни писма, издадени от производителите (или еквивалентни документи), с които се упълномощават официалните представители на производителите, на български език или придружени от превод на български език.

ИНФОРМАЦИОННО ОБСЛУЖВАНЕ

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340,
office@is-bg.net www.is-bg.net
ЕИК: 831641791

Приложение № 2

ОБРАЗЕЦ

ДО
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД
УЛ. „ПАНАЙОТ ВОЛОВ“ № 2
ГР. СОФИЯ

[наименование на участника],

представлявано от [трите имена] в качеството на [длъжност, или друго качество]

с ЕИК […], електронен адрес […], телефон […],

банкови сметки: […]

ОФЕРТА

за

участие в процедура за избор на доставчик с предмет:

„Придобиване на лицензи за платформа за създаване на стратегия за привличане на киберпрестъпници с цел ранно откриване на различните техники и методи на атака за период от 36 месеца за нуждите на „Информационно обслужване“ АД“

След запознаване със запитването за оферта за участвате в процедура за избор на доставчик с предмет: „Придобиване на лицензи за платформа за създаване на стратегия за привличане на киберпрестъпници с цел ранно откриване на различните техники и методи на атака за период от 36 месеца за нуждите на „Информационно обслужване“ АД“ и Количествена и техническа спецификация – Приложение № 1, с настоящата оферта правим следните предложения:

1. Декларираме, че ще изпълним предмета на настоящата процедура, съгласно условията, посочени от Възложителя в запитването за оферта и Количествена и техническа спецификация – Приложение № 1.

2. Предлаганата от нас обща цена за изпълнение предмета на горецитираната процедура, в съответствие с Количествена и техническа спецификация – Приложение № 1 е **в размер на ……..…….. (словом: ……..) лева без ДДС**, формирана както следва:

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340,
office@is-bg.net www.is-bg.net
ЕИК: 831641791

Вид/Продукт	**Количество**	**Единична цена в лв. без ДДС**	**Обща цена в лв. без ДДС**
Лиценз за платформа за създаване на стратегия за привличане на киберпрестъпници с цел ранно откриване на различните техники и методи на атака за 10 симулирани deception крайни-точки, неограничен брой honeypot елементи с включени поддръжка и обновления до последна версия за период от 36 месеца.	30		

3. Декларираме, че ще доставим лицензи за платформа за създаване на стратегия за привличане на киберпрестъпници с цел ранно откриване на различните техники и методи на атака за период от 36 месеца в срок до – …… (……) работни дни /*не повече от 10 (десет) работни дни*/, считано от датата на влизане в сила на договора.

4. Срокът на валидност и поддръжка на лицензите е 36 (тридесет и шест) месеца, считано от датата на приемо-предавателния протокол за доставка.

5. Начин на плащане – извършва се по банков път, в срок до ……(……..……) календарни дни /*не по-малко от 30 (тридесет)* календарни дни/, след подписване на приемо-предавателен протокол за приемане без възражения и забележки от Възложителя и издадена фактура от Изпълнителя.

6. Декларираме, че в предложената цена са включени всички разходи за изпълнение предмета на процедурата.

7. Срокът на валидност на офертата - …….…… календарни дни (*не по- малко от 60 календарни дни*), считано от датата на представяне на офертата.

ПОДПИС

[име и фамилия]

[качество на представляващия участника]

Забележка: *Офертата за участие в процедурата се представя в електронен вид във формат .pdf, подписана с квалифициран електронен подпис.*