Техническа спецификация по обособена позиция № 9 с предмет:

„Доставка на хардуерни устройства и софтуерни пакети за платформа за управление на събития и сигурността на информацията“

1. **Платформа за управление на събития и сигурността на информацията**

Общи изисквания	
REQ.1.	Системата трябва да предоставя управление на всички свои компоненти и административни функционалности посредством web базиран интерфейс.
REQ.2.	Административните правомощия трябва да позволяват дефиниране на достъп до системата според устройства, група от устройства или мрежови диапазон.
REQ.3.	Административните правомощия трябва да позволяват дефиниране на ролево-базиран достъп до различни функционални области на системата. Това включва ограничаване на достъпа до специфична функционалност извън обхвата на потребителската роля. Тази функционалност може да бъде административна, отчетна, филтрираща събития, корелация на събития, достъп до работен плот и др.
REQ.4.	Системата трябва да позволява автоматично откриване на активи, които са обект на защита и наблюдение.
REQ.5.	Системата трябва да позволява автоматична класификация на активите, които са обект на защита.
REQ.6.	Системата трябва да предоставя отворено API за достъп до данните съхраняващи се в базите от данни в системата.
REQ.7.	Системата трябва да предоставя възможност за криптиране на комуникацията между компонентите си.
REQ.8.	Системата трябва да позволява интеграция с външни системи за автентикация.
REQ.9.	Системата трябва да позволява разширена таксонометрия на отчетените събития и описващите ги полета. Потребителите да имат възможност да добавят свои уникални имена на събития, за целите на бъдеща филтрация, доклади или корелация.
REQ.10.	Системата трябва да има възможност за автоматична класификация (tagging) на отчетените събития.
REQ.11.	Системата да предоставя web-базиран графичен интерфейс за управление, анализ и извличане на рапорти.
REQ.12.	Системата да позволява създаване на различни работни плотове според специфичните изисквания на всеки отделен потребител.
REQ.13.	Системата да разполага с набор от преконфигурирани шаблони на работни плотове, които да могат да се използват без допълнителни промени.
REQ.14.	Системата да поддържа база от данни за всички активи открити в информационната инфраструктура. Данните за активите да предоставят важна информация събрана за тях, която включва минимум: системни атрибути, мрежови атрибути и ниво на уязвимост. Системата да позволява корекция на тези атрибути, ако те не могат да бъдат придобити.

REQ.15.	Архитектурата на системата трябва да предоставя възможност за внедряване на всички функционалности за събиране, наблюдение, анализ и управления на журналните събития като цялостно хардуерно решение.
REQ.16.	Архитектурата на системата трябва да предоставя възможност за внедряване на функционалностите за автоматизиране на процесите за реакция при инциденти във виртуална среда.
REQ.17.	Архитектурата на системата да гарантира интегритет на събраните данни (журнални записи).
REQ.18.	Архитектурата на системата трябва да може да предоставя разпределен модел на корелация на активности събрани от различните ѝ източници. Пример: покажи X грешни опити за въвеждане на парола за даден потребител, като данните за тези опити са събрани от всички компоненти.
REQ.19.	Системата да предоставя автоматизиран процес за архивни копия (конфигурации и събрани журнални записи) и тяхното възстановяване.
REQ.20.	Системата трябва да предоставя автоматизирани проверки на работоспособност и при възникване на проблем да изпраща нотификация.
REQ.21.	Системата трябва да позволява съхранение на събраните журнални записи върху външни системи (независимо от производителя) за съхранение.
REQ.22.	Системата трябва да позволява разширени възможности за търсене, анализ и централизирани справки с журналните записи, които се съхраняват на върху външни системи за съхранение.
REQ.23.	Системата да предоставя възможност за компресия на събраните журнални записи.
REQ.24.	Системата да позволява стандартизирани методи за събиране на журнални записи като минимум: Syslog (TCP/UDP), SNMP, JDBC, OPSEC LEA, SDEE, WMI, FTP/SFTP/SCP като място за съхранение на журнални записи.
REQ.25.	Системата трябва да позволява нормализация на базовите събитийни полета. В това число: потребителски имена, IP адреси, имена на хостове, източници на журнални записи.
REQ.26.	Системата трябва да позволява анализ на събитията в близко до реалното време.
REQ.27.	Системата трябва да позволява анализ за събитията в дълъг период от време, показване на базова линия (baseline) и прогноза (trend) върху тези събития.
REQ.28.	Системата трябва да създава аларми базирани на наблюдавани аномалии и поведенчески промени в събитията свързани със сигурността.
REQ.29.	Системата да предоставя възможност за отчет/рапорт на всички компоненти, подлежащи на управление през графичният потребителски интерфейс.
REQ.30.	Системата да притежава конфигурируема подсистема/модул за създаване на отчети, позволяваща гъвкавост и промени на генерираните отчети.
REQ.31.	Системата да позволява създаване на отчет за определен интервал от време: час, ден, седмица месец или на специфично зададен период.
REQ.32.	Системата да позволява направа на шаблони за лесно изготвяне и предоставяне на отчети за нуждите на широка гама от нива както оперативни така и ръководни
REQ.33.	Системата да предоставя възможност за алармиране базирано на засечени заплахи за сигурността въз основа на наблюдаваните устройства.

REQ.34.	Системата да предоставя възможност да корелира информация събрана от различни компоненти на системата.
REQ.35.	Системата да предоставя възможност за алармиране базирано на установени политики.
REQ.36.	Системата да предоставя възможност за алармиране базирано на претегляне, което ще позволи залагане на приоритизация.
REQ.37.	Системата да позволява изпращане на аларми към външни системи посредством e-mail, SNMP и Syslog.
REQ.38.	Системата да има вграден инструмент през който потребителите да могат да описват защо дадена аларма е false positive и респективно тези данни да се използват за намаляване на нивото на фалшивите аларми в последствие.
REQ.39.	Системата да позволява корелация на свързани помежду си събития и представянето им като един инцидент.
REQ.40.	Системата да има възможност за интеграция с външни източници на информация от трети страни свързана със заплахи (географско позициониране, ботнет канали, враждебни мрежи). Получената информация да може да се използва по автоматизиран начин.
REQ.41.	Системата трябва има възможност да алармира когато има прекъсване в събирането на журнални записи от устройствата под наблюдение. Потребителите на системата да имат възможност да дефинират времевият интервал през който не се наблюдава активност от наблюдаваните устройства. Пример: ако журналните записи не са изпратени от дадено устройство в рамките на X минути да се създаде аларма.
REQ.42.	Системата трябва да има възможност за предприемане на действия при получаване на сигнал. Системата трябва да има възможност за иницииране на персонализиран скрипт, който може да бъде параметризиран по атрибути от събитията или изпращане на email съобщение, syslog, SNMP trap.
REQ.43.	Системата за събиране, наблюдение, анализ и управления на журнални събития трябва да има интегрирана възможност за получаване на информация за заплахи предоставяна от производителя.
REQ.44.	Системата трябва да позволява исторически анализ на журнални записи, напр. събития и потоци от минало време и ново добавени правила.
REQ.45.	Системата трябва да има възможност да корелира потоци от данни от трети страни. Тези данни на трети страни трябва се актуализират автоматично от системата. Системата трябва да предоставя възможност за обмен на стандартизирана информация като STIX или TAXII.
REQ.46.	Системата трябва да има възможност за създаване и поддържане на списък с всички активи на дадена организация. За всеки един актив да може да се определя теглови коефициент и да бъде асоцииран с ползвателя и географската му локация.
REQ.47.	Системата трябва да може при интеграция с решение за управление на уязвимости (Vulnerability Management) да обединява и информация за уязвимостите на даден актив.
REQ.48.	Системата трябва да позволява определяне на ниво на достоверност на всеки един източник на журнални записи, което да може да се взима в предвид при финалното определяне на приоритета на даден инцидент по сигурността.

REQ.49.	Системата трябва да предоставя вградени работни процеси, които улесняват и насочват действията на служители, отговарящи за сигурността.
REQ.50.	Системата трябва да има вграден модул, който да позволява назначаване на даден инцидент по сигурността на определен потребител на системата.
REQ.51.	Всеки един потребител трябва да има възможност да види всички свой (назначени на него) инциденти по сигурността подредени по определен приоритет за обработка.
REQ.52.	Всеки един потребител трябва да има възможност да обработва назначените по инциденти по сигурността и съответно миниум да може да ги отхвърля, наблюдава, конфигурира и коментира нотификации.
REQ.53.	Системата трябва да предоставя възможност за интеграция със система за управление на инциденти (trouble ticketing).
REQ.54.	Системата да предоставя механизъм за прихващане на всички релевантни аспекти свързани с инцидент в сигурността в обединено логическо представяне.
REQ.55.	Системата да предоставя механизъм за добавяне на коментари в събраната и обособена логически информация за текущ инцидент в сигурността.
REQ.56.	Системата да предоставя механизъм за откриване на инциденти в сигурността на база широк спектър от атрибути свързани с него като: IP адрес, потребителско име, MAC адрес, източник на журнален запис, правило за корелация и др.
REQ.57.	Системата да позволява събиране на журнални записи от Microsoft базирани сървърни крайни устройства.
REQ.58.	Системата да позволява събиране на журнални записи от Linux/Unix базирани сървърни крайни устройства.
REQ.59.	Системата да позволява събиране на журнални записи от бази от данни като: • MSSQL Server; • Oracle; • IBM DB2; • Sybase; • IBM Informix
REQ.60.	Системата да позволява събиране на журнални записи от системи за активно наблюдение на бази от данни.
REQ.61.	Системата да позволява събиране на журнални записи от системи за управление на идентичности и достъп (Identity and access Management).
REQ.62.	Системата трябва да предоставя механизъм за извършване на анализ на поведението на потребителите, с цел своевременно откриване на вътрешни заплахи за сигурността и компрометирани данни за автентикация.
REQ.63.	Системата трябва да предоставя възможност за анализ на поведението на потребителите въз основа на събития, които включват идентичност на потребителите. Системата трябва допълнително да осигури възможности за машинно самообучение, базирано на анализ на поведението на потребителите. Функцията за анализ на поведението на потребителите трябва

	да бъде интегрирана в системата за събиране, наблюдение, анализ и управления на журнални събития в една конзола.
REQ.64.	Системата да разполага с възможност за разширяване на функционалността, чрез добавяне на готови приложения и функции, в потребителския интерфейс, представени и налични за сваляне в специализиран портал на проиводителя.
REQ.65.	Системата трябва да предоставя възможност за разработване на допълнителни функции и приложения.
REQ.66.	Системата да позволява събиране на журнални записи от директориини продукти (AD, LDAP и др.).
REQ.67.	Системата да позволява събиране на журнални записи от минимум следните устройства/приложения: • Cisco Switches; • Cisco Routers; • Cisco ASA; • Cisco Nexus; • Cisco ACS; • Cisco Wireless LAN Controllers; • Apache HTTP Server; • Check Point Firewalls; • Citrix NetScaler; • Extreme Matrix Router; • Extreme Extreme Ware; • F5 ASM; • F5 BIG IP; • HP ProCurve; • HP-UX; • Juniper Router; • Juniper Firewalls; • Microsoft Exchange; • Microsoft IIS; • Microsoft Hyper-V; • Microsoft Endpoint Protection; • Microsoft DHCP Server; • Microsoft ISA; • Microsoft SharePoint; • IBM WebSphere; • Oracle BEA WebLogic; • Palo Alto Networks; • Radware DefensePro;

	• Arbor Networks; • RSA Authentication Manager; • VMWare ESX и ESXi; • VMWare vCenter.
REQ.68.	Системата да позволява събиране на журнални записи от водещи в индустрията скенери за уязвимости като: • Nessus; • Nmap; • Qualys; • Rapid7 Nexpose
REQ.69.	Системата трябва да предоставя възможност за бъдещо разширяване с компоненти за наблюдение на мрежовия трафик на ниво Layer 7.
REQ.70.	Системата трябва да бъде доставена с възможност за събиране на поточна информация от мрежовите елементите (network flows) поддържайки следните стандарти: • Cisco Netflow (v5, v7, v9), • IPFIX, • JFlow, sflow
REQ.71.	Системата трябва да бъде доставена с модул за сканиране, откриване и управление на уязвимостите чрез собствена вградена функционалност, същевременно трябва да позволява събиране на информация от водещи в индустрията скенери за уязвимости като: • Nessus; • Nmap; • Qualys; • Rapid7 Nexpose.
REQ.72.	Системата трябва да има възможност за надграждане с функционалности за оценка на риска за критични активи чрез добавяне на допълнителни компоненти.
REQ.73.	Системата трябва да бъде доставена с компоненти даващи разширени възможности за автоматизиране на процесите за реакция при инциденти като: • Динамични инструменти “playbooks”, които автоматично се адаптират към инцидентите в реално време. • Визуални работни процеси, които позволяват да се организират ответни мерки срещу възникнали инциденти. • Визуализация на инцидентите показващи връзки между артефакти за инциденти или индикатори за компромис (IOCs) и инциденти в средата на организацията. • Времево базирани правила в работните процеси (timers). • Управление на потребителите и разделяне на данните между различни екипи по целесъобразност. Ограничаване на достъпа до чувствителни данни чрез работни пространства и адаптивен контрол на достъпа, базиран на роли.

REQ.74.	Системата трябва да има възможност за предоставяне на множество работни плотове за управление, които могат да бъдат персонализирани, за да отговарят на специфичните изисквания на различни потребители на системата.
REQ.75.	Администраторът трябва да може да дефинира достъп базиран на роли до различни функционални области на системата.
REQ.76.	Системата трябва да осигури удостоверяване на потребителите чрез интеграция с активна директория (Active Directory).
REQ.77.	Системата трябва да поддържа база данни за инциденти. Потребителят трябва да може да търси в тази база данни.
REQ.78.	Системата трябва да поддържа история на активността на потребителя за всеки инцидент.
REQ.79.	Системата трябва да може да поддържа съхраняването на досиета свързани с инциденти, които не са ограничени до образци на зловреден код, журнални записи, снимки от екрана.
REQ.80.	Системата трябва да предоставя възможност за съпоставяне на артефактите при потенциално различни инциденти.
REQ.81.	Системата трябва да осигурява визуализация на индикатори за компромис (IOCs), за да се идентифицират по-лесно взаимовръзките.
REQ.82.	Системата трябва да има възможност за корелация наданни по сигурността от трети страни.
REQ.83.	Системата трябва да осигурява конфигурируем механизъм за създаване на персонализирани отчети.
REQ.84.	Системата трябва да осигурява възможност за добавяне на персонализирани работни процеси чрез web-базиран графичен интерфейс
REQ.85.	Системата трябва да осигури възможност за оркестриране и автоматизиране чрез интеграция с персонализирани системи на трети страни.
REQ.86.	Системата трябва да има вградени възможности за интеграция между компонентите за реакция при инциденти и компонентите за събиране, наблюдение, анализ и управления на журнални събития.
REQ.87.	Системата трябва бъде скалируема и да предоставя възможности за разрастване безда е необходима пренастройка на инсталираната среда.
REQ.88.	Системата трябва притежава вградена възможност за създаване на резервно копие на конфигурацията върху външни носители през графичния административен интерфейс, както и иницииране на възстановяване от резервно копие през същия интерфейс.
REQ.89.	Системата трябва да може да работи в режим “High Availability” при бъдещо добавяне на идентичен компонент в отдалечена локация и прехвърляне на работата върху него в случай на нужда.
REQ.90.	Системата трябва да се достави с цялото необходимо хардуерно и лицензно обезпечаване от производителя на платформата за наблюдение и обработка, с капацитет минимум: • 10 000 събития в секунда (Events Per Seconds); • 700 сесии в секунда (Flows per Second); • 760 сканирани актива (IP адреси) за уязвимости; • Без ограничения за некорелираните събития

REQ.91.	Минимум един хардуерен компонент със следните минимални характеристики: • RAM: 128 GB; • HDD: 7,2K rpm с общ капацитет преди групиране в RAID поне 60 TB; • Networking: • 2 броя 16 Gbps Fiber Channel HBA • 2 броя 10 Gbps SFP + Ethernet ports • Резервирани захранващи блокове.
REQ.92.	Системата трябва да се достави с цялото необходимо лицензно обезпечаване за компонентите за реакция при инциденти, с капацитет минимум: • 3 броя оторизирани потребители на системата • 3000 месечни действия
Гаранция и поддръжка:	
REQ.93.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.94.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.95.	Получаване на нови версии на софтуера - минимум 5 (пет) години.