

ПЕРСПЕКТИВНИ СПЕЦИАЛИЗИРАНИ СИСТЕМИ ЗА ОТКРИВАНЕ И РЕАГИРАНЕ НА ЗАПЛАХИ В КИБЕРСИГУРНОСТТА

Цветелина Симеонова

Promising Specialized Systems for Detecting and Responding to Threats in Cybersecurity

Tsvetelina Simeonova

Резюме: Цел на настоящата работа е изследване на перспективни специализирани системи за откриване и реагиране на заплахи в киберсигурността. За постигането на целта е направен анализ и са систематизирани характеристики на специализирани системи за откриване и реагиране на заплахи. Приноси моменти са направените съпоставки между различните варианти на използване на системите и някои възможни взаимозависимости между тях за предоставяне на конвергентни услуги.

Ключови думи: киберсигурност, конвергенция, откриване и реакция

Abstract: The aim of this work is to study promising specialized systems for detecting and responding to threats in cybersecurity. To achieve this goal, an analysis has been made and the characteristics of specialized systems for detecting and responding to threats have been systematized. The comparisons made between the different options for using the systems and some possible interdependencies between them for providing convergent services are of particular interest.

Keywords: cybersecurity, convergence, detection and response

Въведение

Важен аспект при развитието на цифровите инфраструктури, особено с навлизането на Интернет, облачните технологии, мобилността и Интернет на нещата IoT (Internet of Things) се оказва киберсигурността. Въвеждането на новите технологии разширява повърхността за атака и поради това киберсигурността все повече се превръща в територия на бизнеса [1, 2, 3, 4, 5, 6].

В края на миналия век продуктите за киберсигурност започнаха да запълват стелажите до достигане на точката, в която сложността, като резултат от неуточненост и неуреденост на присъстващата функционалност в отделните продукти, поражда объркване в определени случаи на използване на технологиите за откриване и реагиране на заплахи към киберсигурността и затруднява наблюдението и управлението на огромния брой сигнали за тревога (alerts) идващи от различни системи.

Множеството предупредителни сигнали на системно ниво, както и от крайни точки, генерирани ежедневно, трябва да бъдат приоритизирани, разследвани и смекчени. В тази връзка предупрежденията по отношение на киберсигурността си остават предизвикателство за операциите по сигурността. Конвергенцията на разнородни технологии е общо направление, което следва новонавлизащи иновативни технологии с цел предоставяне на потребителите на нови и конвергентни услуги за киберсигурност. Решаващо се оказва доколко добре дадено решение се справя с удовлетвореността на потребителите и допринася за увеличаване на бизнес печалбите, което предизвиква трансформации и конвергенция на технологиите.

Характерна черта на голяма част от съществуващите технологии за защита, независимо от различните случаи на използване е, че използват принципите на широко разпространените

**ПЕРСПЕКТИВНИ СПЕЦИАЛИЗИРАНИ СИСТЕМИ ЗА ОТКРИВАНЕ И РЕАГИРАНЕ НА
ЗАПЛАХИ В КИБЕРСИГУРНОСТТА
ЦВЕТЕЛИНА СИМЕОНОВА**

наследени системи, например "системи за откриване/ предотвратяване на проникване" IDS (Intrusion Detection System) и IPS (Intrusion Prevention System). Новонавлизащите технологии за защита се базират на специфична специализирана насоченост, съчетано с основна функционалност, а именно "откриване и реакция" (Detection and Response).

1. Специфика на тясно специализирани системи за откриване и реагиране на заплахи

Решението "Откриване и реагиране на заплахи" TDR (Threat Detection and Response) е специфичен термин, тъй като множество доставчици предлагат различни инструменти съответстващи на тази терминология. TDR може също да се разгледа като по-широк и разнообразен набор от инструменти, технологии и процеси за предотвратяване на кибератаки, използващи данни за осигуряване на сигурност в реално време на различни организации. Тази категория от решения за откриване и реагиране на заплахи TDR обхваща различни специфични продукти, в които присъства функционалност за сканиране на уязвимости, поведенчески анализ, разследване и преследване на заплахи и тестове за проникване [7].

Най-често използваните приложения на TDR са:

- **TDR на Крайна точка** (endpoint TDR) по същество е модифициран подход към решението "Откриване и реакция на крайна точка" EDR (Endpoint Detection and Response). Традиционният EDR е проектиран да записва възможно най-много данни за това какво се случва в крайната точка. Това създава ситуация, при която много от данните, записвани от EDR инструментите, може да се възприемат като ненужни. TDR за разлика от EDR записва данни само след като реши, че има възникнала потенциална заплаха, или записва само извадка от процеси и събития, които е най-вероятно да разкрият заплаха. По отношение на реакцията когато бъде открита заплаха, тази форма на TDR често функционира като традиционния EDR.

- **Аналитичен TDR** (analytical TDR) използва съществуващи данни за анализ на възможности за откриване и реакция. Аналитичният TDR подход използва „големи данни“ и прилага анализи за откриване на заплахи. След като бъде открита заплаха, като реакция най-напред се задейства предупреждение и проблемът се насочва за разрешаване.

Решението "Откриване и реакция на крайна точка" EDR (Endpoint Detection and Response) непрекъснато наблюдава крайни точки (устройства, свързани към мрежата), за да открие злонамерено поведение или зловреден софтуер. Идеята при EDR е, че всяка крайна точка свързана към мрежата е потенциален вектор за навлизане на нападател. EDR системите помагат на потребителите да реагират на заплахи, а с някои инструменти този процес е автоматизиран [8].

Софтуерът на EDR агент се внедрява в крайни точки на организацията, записва извършващата се дейност, след което тези записани данни се използват, за да се открият потенциални заплахи.

EDR често се нарича естествена еволюция на антивирусния софтуер, тъй като и двата инструмента изпълняват подобни функции. Традиционната антивирусна програма обикновено извършва "откриване, базирано на сигнатури" (signature-based detection) за да открие известни заплахи. EDR използва "откриване, базирано на поведение" (behavior-based detection), за да открива нововъзникващи атаки, като усъвършенствани постоянни заплахи APTs (Advanced Persistent Threats) и специфичен злонамерен софтуер, а традиционната антивирусна програма обикновено не го прави.

EDR също събира и предоставя информация, необходима за разследване (криминалистичен анализ) на всяка идентифицирана злонамерена дейност, като надхвърля действията, предприемани от антивирусната програма.

Съществуващите EDR решения имат специфика - някои EDR имат антивирусна функционалност, а други са проектирани да откриват това, което традиционната антивирусна програма не може.

EDR софтуерът може да бъде компонент на антивирусни продукти от следващо поколение.

Един недостатък на EDR е, че софтуерът е ограничен само до крайни точки. За цялостен поглед върху съвременните хибридни среди и за най-ефективни способности за откриване и реагиране трябва да се събират, анализират и корелират данни от много различни източници.

През последните години технологията EDR беше включена в други платформи и инструменти, поради което тя е по-малко използвана като самостоятелна опция за киберсигурност.

Причина за това е осъзнаването от организациите, че заплахите трябва да се наблюдават и спират, преди да достигнат до крайна точка, етап на ескалация. Откриването на заплахи в крайни точки е важно за изясняване на цялостната картина при инциденти, но се счита за твърде закъсняло решение, в случай на кибератака.

Друг аспект е категоризирането на EDR като част от XDR (Extended Detection and Response). Междувременно доставчиците на EDR са добавили допълнителни функции за телеметрия, а доставчиците на XDR са добавили функции за обща наличност. На база на добавената функционалност е налице тенденцията за сближаване на EDR и XDR.

Решението "Мрежово откриване и реакция" NDR (Network Detection and Response) се отнася за защита на мрежовия периметър срещу насочени кибератаки и е фокусирано към откриване базирано на наблюдавани данни от мрежовия трафик на дадена организация [7]. Една от характеристиките на NDR е използването на изкуствен интелект AI (Artificial Intelligence) при откриването на кибератаки. Обобщено може да се каже, че NDR са усъвършенствани системи за откриване на проникване (или $NDR \approx IDS/IPS$).

Доставчиците на NDR може да имат множество подходи за това как да наблюдават и анализират този трафик, но като цяло е необходим мрежов сензор. Това обикновено е физическо или виртуално мрежово устройство или комбинация от двете. Тези сензори се включват в мрежата наблюдавайки трафика, или докато трафикът се насочва към местоназначението си, или в огледална конфигурация към която се препраща за анализ копие на трафика.

Откриванията при NDR често се базират на обобщен изглед на околната среда. Вместо да открива заплахи въз основа на необичайни процеси или на детайлизирани събития, както при EDR, NDR търси потенциални заплахи въз основа на аномално конфигурирани или неототоризирани протоколи, аномалии при използване на портове, необичайно време и размери на трансфер и др.

NDR може да задейства предупреждения, да намали трафика на сървъра, да постави устройство под карантина и да генерира доказателства при криминалистични разследвания.

Сигурността на мрежата стана по-важна през последните години, тъй като източниците на заплахи са насочили погледа си към тази част от сигурността на инфраструктурата, особено към разширяващите се облачни мрежи.

Едно ключово предимство е, че не се разчита на внедрен агент във всяка крайна точка. Това го прави много подходящ за среди, в които EDR може да не е в състояние да покрие всяка система.

**ПЕРСПЕКТИВНИ СПЕЦИАЛИЗИРАНИ СИСТЕМИ ЗА ОТКРИВАНЕ И РЕАГИРАНЕ НА
ЗАПЛАХИ В КИБЕРСИГУРНОСТТА
ЦВЕТЕЛИНА СИМЕОНОВА**

Друго предимство е, че NDR може да открие и да реагира на неоторизирани устройства.

Решенията за "разширено откриване и реакция" XDR (Extended Detection and Response) се развиват от системите за "откриване и реакция на крайна точка" EDR (Endpoint Detection and Response). Разширявайки се отвъд крайната точка, XDR решенията събират информация от мрежи, сървъри, облачни приложения и др. XDR централизирано обработва предупрежденията за сигурност от няколко съществуващи инструмента за сигурност в мрежата (антивирус, EDR, NDR, IDS/IPS и др.). След това сигналите се обработват и анализират от XDR за откриване на по-сложни атаки [7, 8, 9].

XDR е единична платформа, която може да възприема данни от агент на крайна точка, информация на ниво мрежа и в много случаи от регистрационни файлове на устройството. Тези данни са свързани (корелирани) и откриванията могат да възникнат от един или много източници на телеметрия за да се постигне цялостен изглед за откриване на заплахи. Тези инструменти могат да видят какво се случва не само в крайните точки, но и между крайните точки.

Предимството на XDR е рационализирането на функциите на ролята на анализатора, като позволява да се преглеждат по-точно засичанията и да се предприемат ответни действия от една централна конзола за управление. Този подход предлага по-кратко време за оценяване, по-опростено обучение и по-кратки времена за реакция.

Случаите на използване на XDR включват търсене на заплахи в реално време, (което помага да се определи какво е реално или не в сценариите за атака), и преглед на индикатори за компрометиране IoCs (Indicators of Compromise) с цел по-задълбочено разследване и по-бърз, автоматизиран отговор.

Някои доставчици на XDR предоставят платформи, които работят само със собствения пакет инструменти на този доставчик, докато други предоставят отворени XDR опции, които се интегрират по-широко с трети страни за по-голяма видимост и подобрени възможности за откриване и реагиране.

Решенията XDR се различават от Системата за информационна сигурност и управление на събития SIEM (Security Information and Event Management) и от Оркестрация на сигурността, автоматизация и реакция SOAR (Security Orchestration, Automation and Response) по нивото на интеграция при внедряване и способността да се справят с откриването на заплахи и реакциите при инциденти.

Някои XDR платформи (особено базирани на EDR решения), не отговарят на всички нужди на различни SIEM или случаи на използване за анализ на сигурността, включително съответствие, докладване, сортиране, корекция и менажиране на уязвимости. Платформата SIEM + XDR включва дългосрочно запазване на данни и автоматизиран отговор за поддръжка на случаи на използване в по-широк аспект, включително изисквания за съответствие и киберзастраховка.

Решението "Управлявано откриване и реакция" MDR (Managed Detection and Response) извършва проактивно наблюдение на киберсигурността на компютърни мрежи. В един MDR екип, за да осигурят защита от кибератаки, работят заедно специалисти с различни профили: специалисти по откриване на прониквания, преследвачи на киберзаплахи, специалисти по анализ на зловреден код и др.

Една MDR услуга използва една или повече технологии за киберсигурност, например някои MDR използват само EDR, други използват само NDR, а други използват комбинация от технологии.

Това позволява да се избере MDR, който отговаря на конкретните нужди. MDR се различава съществено от другите решения, тъй като е решение за менажирана услуга, което често комбинира технологии с външни анализатори (аутсорсинг услуга) за откриване и реагиране на злонамерено поведение в мрежа. Доставчиците на MDR

предлагат технология, която обхваща крайни точки, мрежи, облачни услуги, оперативна технология и Интернет на нещата IoT (Internet of Things), както и събиране на данни от други източници като регистрационни файлове и данни.

MDR може да помогне за осигуряване на ограничителни действия, като част от реакцията при инцидент, за да помогне на клиентите без функционалност на вътрешни оперативни центрове за сигурност SOC (Security Operations Centers) да осигурят незабавни действия.

От друга страна, MDR изнесен като аутсорсинг услуга все още изисква локален контекст, за да завърши отстраняването на инцидента, тъй като няма същите вътрешни познания за средата на клиента като локалния IT екип.

Има две основни категории решения за MDR: Фокусиран върху продукта MDR (Product-focused MDR) и Доставчик на MDR "за чиста игра" (pure-play MDR provider).

MDR е естествена еволюция на традиционния подход за управление на киберсигурността, под формата на Център за операции по сигурността. Центърът за операции по сигурността е пасивен и анализаторите на центъра се намесват само при подаване на предупреждение. Често обаче, когато се генерира сигнал, вече е късно. Следователно MDR е много по-адаптиран към текущото управление на мрежовата сигурност.

Решението за "Откриване и реакция в облак" CDR (Cloud Detection and Response), наричано също "Откриване и реакция на заплахи в облак" CTDR (Cloud Threat Detection and Response), предоставя възможности за предотвратяване, откриване и реагиране на заплахи, пригодени за мултиоблачни среди [10].

CDR по принцип използва технология без агенти, за да предложи защита, видимост в реално време и идентифициране на заплахи, уязвимости, неправилни конфигурации и пропуски в съответствието, без да пречи на функционирането. CDR предоставя:

Гъвкаво внедряване: Поддържа опции, базирани на агенти и без агенти, позволявайки безпроблемна интеграция в облачни среди.

Централизирано табло за управление: Предлага унифициран изглед на заплахи, уязвимости и състояние на съответствие във всички облачни активи.

Наблюдение в реално време: Непрекъснато проследява натоварванията, конфигурациите и дейностите за откриване на рискове като злонамерен софтуер, рансъмуер и нарушения на данни.

Автоматизирана реакция: Предоставя полезна информация/прозрения и автоматизация, за да позволи бързо ограничаване на заплахи.

Приоритизиране на риска: Оценява и класира заплахите въз основа на тяхното потенциално въздействие, като помага на екипите по сигурността да се съсредоточат върху критични проблеми.

2. Специфика на комплексни специализирани системи за откриване и реагиране на заплахи

Система за информационна сигурност и управление на събития SIEM (Security Information and Event Management)

Решенията за SIEM съществуват от десетилетия, с различна степен на функционалност в зависимост от продукта или доставчика. SIEM е централизиран инструмент за управление на регистрационни файлове (centralized log management tool), който се интегрира с приложения, системи, сървъри и т.н., за да събира данни от всяка услуга (log files).

**ПЕРСПЕКТИВНИ СПЕЦИАЛИЗИРАНИ СИСТЕМИ ЗА ОТКРИВАНЕ И РЕАГИРАНЕ НА
ЗАПЛАХИ В КИБЕРСИГУРНОСТТА
ЦВЕТЕЛИНА СИМЕОНОВА**

SIEMs се използват за анализ на събития за сигурност, за да помогнат при разследване, за ранно откриване на заплахи и за реакция при инциденти. Те също така поддържат съответствие на случаи на използване, тъй като много регулаторни рамки за данни изискват от организациите да поддържат одитни регистрационни файлове (audit logs) за една година или повече в зависимост от рамката и индустрията.

SIEMs могат да бъдат хоствани в облака или локално. Модерният SIEM трябва да може да обслужва облачни данни и да открива ранни признаци на злонамерено поведение, като опити за неоторизиран достъп и др.

Традиционните SIEM могат само да събират информация от регистрационни файлове, оставяйки на потребителите да изградят допълнителна функционалност (правила за откриване, анализиране и т.н.) за да извлекат някаква стойност за сигурността от решението.

По-модерните SIEM са разработени с предварително изграден "набор от откривания" и наръчници за улесняване на потребителите за по-бърз отговор на заплахи.

Самостоятелните традиционни SIEMs може да изискват големи екипи от специалисти по сигурността за внедряване и стартиране на функционирането.

Усъвършенстването на SIEM с използване на "разширено откриване и реакция" XDR (Extended Detection and Response) може да автоматизира откриването и реакцията за използване от по-малки екипи, като същевременно запазва исторически данни, за да помогне за спазването на множество разпоредби за съответствие (като регистриране, преглед на регистрационни файлове, откриване на аномалии и др.).

Модерният SIEM + XDR интегрира широко различни инструменти, включително EDR, за да осигури по-добър мониторинг, автоматично да съпостави данните и да изпраща констатации с отчитане на контекста за индикатори с висока степен на увереност за заплахи в конкретна среда.

Оркестрация на сигурността, автоматизация и реакция SOAR (Security Orchestration, Automation and Response)

Традиционните SIEMs често изискват много ръчна работа отнемаща време за изпълнение на задачи за сигурност, например настройка на правилата за откриване, за да се предотвратят фалшиви положителни резултати, както и претоварване от множеството предупреждения. Също така, други ръчни задачи включват корелация на данни, която включва търсене в регистрационни файлове и сравняване на данни от различни източници, за да се определи дали има достоверна заплаха.

Решенията SOAR се развиха като начин да се помогне на анализаторите в Центъра за операции по сигурността SOC (Security Operations Center) да са по-ефективни, позволявайки по-автоматизирано приоритизиране и обработка на събития и инциденти, свързани със сигурността.

Ключовите възможности на SOAR решенията включват:

• Оркестрация:

- Интегриране на различен софтуер като защитни стени, SIEMs, "откриване и реакция на крайни точки" EDR (Endpoint Detection and Response) и външни канали за откриване на заплахи, в опит да се съберат всички платформи за киберсигурност в един "прозорец".
- Предварително изградени автоматизирани работни процеси за рационализиране на процеса на реагиране на предупреждения

• Автоматизация:

- Наръчниците представляват ръководства за процедури за реакция, на база на които могат да се автоматизират и рационализират операциите по сигурността, за да се намали ръчното разследване и вземане на решения по време на стресови моменти.

- Натрупване на доказателства или автоматично попълване на подходящи данни, за да се осигури по-полезен, приложим контекст за реакция. Например платформата може да насочи потребителите към засегнат IP адрес или хост, който трябва да проучат.

- Автоматизирани блокиращи действия, като например динамични списъци за блокиране, които се интегрират със защитни стени, за да идентифицират и автоматично блокират достъпа от известни “недоверени” източници на трафик, използвайки актуализирани емисии за разпознаване на заплахи.

• **Отговор (реакция):**

- Случаите на използване на SOAR често включват реакция след инцидент с възможности като докладване, анализ и мениджмънт на конкретния случай.

- Автоматизирана реакция, като ограничаване или изолиране на крайна точка, е друг начин за ускоряване на реакцията при заплаха, прекъсвайки достъпа до мрежата на засегнато устройство.

SOAR инструментите често се използват за подобряване на традиционните SIEM платформи на които липсват тези възможности. Въпреки това, много съвременни SIEM + XDR платформи консолидират много от изброените възможности за реагиране в едно интегрирано решение, елиминирайки необходимостта от закупуване и свързването им заедно на различни инструменти за откриване и реагиране.

Център за операции по сигурността SOC (Security Operations Center)

Центърът за операции по сигурността се управлява от екип за операции по сигурността SecOps (Security Operations), който непрекъснато наблюдава, анализира и реагира на инциденти, свързани със сигурността. Центърът приема данни от мрежите, устройствата, сървърите и т.н.. След това се изисква анализаторите на центъра да определят следващите стъпки за възстановяване при възникнала необходимост. Много организации не могат да си позволят да поддържат вътрешен SOC или персонал за SecOps екип, тъй като е скъпо и отнема време да се наемат, обучават, и поддържат опитни специалисти по сигурността. В тази връзка индустрията на информационната сигурност създава услуги за управлявано откриване и реакция MDR (Managed Detection and Response), които имат за цел да подобрят или заменят SOC.

3. Особенности при развитието и съвместната работа на специализирани системи за откриване и реагиране на заплахи

Традиционните решения за откриване и реакция са изначално предназначени предимно за локални среди, докато съвременните облачни екосистеми се нуждаят от повече скалируемост и гъвкавост. За разлика от наследените системи, решението CDR е специално създадено за облачни среди, като използва ресурсите си за откриване на заплахи в реално време и предоставя възможности за автоматизирана реакция, които отговарят на динамичните нужди на съвременните облачно базирани инфраструктури.

CDR и Откриване и реакция на крайна точка EDR (Endpoint Detection and Response)

CDR и EDR изпълняват различни, но допълващи се роли в киберсигурността. CDR е фокусиран върху откриването и реагирането на заплахи в облачни среди, докато EDR е съсредоточен върху защитата на отделни крайни точки. Заедно те осигуряват цялостен

**ПЕРСПЕКТИВНИ СПЕЦИАЛИЗИРАНИ СИСТЕМИ ЗА ОТКРИВАНЕ И РЕАГИРАНЕ НА
ЗАПЛАХИ В КИБЕРСИГУРНОСТТА
ЦВЕТЕЛИНА СИМЕОНОВА**

подход за сигурност, като покриват специфични за облака заплахи и заплахи на ниво крайна точка, осигурявайки цялостна защита в инфраструктурата на организацията.

CDR и Система за информационна сигурност и управление на събития SIEM (Security Information and Event Management)

CDR и SIEM се допълват взаимно за да осигурят цялостно решение за сигурност:

Интегрирани данни: CDR подава специфична за облака телеметрия и прозрения в SIEM, обогатявайки техния набор от данни и подобрявайки цялостните способности за откриване на заплахи и намиране на корелации.

Координирана реакция: Автоматизираната реакция на CDR на специфични за облака заплахи може да задейства предупреждения или действия в рамките на SIEM, позволявайки унифицирана и координирана реакция при инциденти със сигурността във всички среди.

Унифицирана видимост: CDR и SIEM заедно предоставят пълен поглед върху състоянието на сигурността на организацията, осигурявайки последователно наблюдение, откриване и реакция в облачни, хибридни и локални инфраструктури.

CDR и Мрежово откриване и реакция NDR (Network Detection and Response)

CDR и NDR работят заедно, като предлагат специализирано откриване на заплахи и реакция както на облачно, така и на мрежово ниво, осигурявайки по-устойчива и цялостна стратегия за киберсигурност в дигиталната екосистема на организацията.

CDR идентифицира заплахи, специфични за облака, докато NDR открива заплахи, разпространяващи се в мрежите, осигурявайки цялостно покритие на облачния и мрежовия слоеве. Прозрения от CDR могат да информират NDR за специфични за облака заплахи и обратно, позволявайки координирана и по-бърза реакция при инциденти в цялата среда.

CDR и Платформа за защита на натоварванията на облака CWPP (Cloud Workload Protection Platform)

Решението CDR е специализирано в откриването и реагирането на заплахи в цялата облачна инфраструктура. От своя страна, CWPP защитава специфични "облачни натоварвания", например приложения, контейнери, виртуални машини и др. CWPP предлага набор от мерки за сигурност, включително управление на уязвимостите, защита по време на изпълнение и управление на съответствието. Заедно CDR и CWPP предлагат цялостен подход към облачната сигурност.

CWPP и CDR се допълват взаимно, тъй като се занимават с различни аспекти на облачната сигурност, осигурявайки по-всеобхватна стратегия за защита. CWPP гарантира, че работните натоварвания са сигурни, а CDR наблюдава по-широката облачна среда за всякакви заплахи или аномалии, осигурявайки защита "от край до край".

CDR и Разширено разследване на сигурността и автоматизиран мениджмънт XSIAM (Extended Security Intelligence and Automation Management)

CDR допълва решението разширено разследване на сигурността и автоматизиран мениджмънт XSIAM, като подобрява възможностите за предотвратяване, откриване и реакция на заплахи за облачни среди.

Заклучение

Цел на настоящата работа е да се изяснят подходите за развитие на различни инструменти на киберсигурността. Като резултат е направен подбор и анализ на съвкупност от различни технологични решения със специфична насоченост.

Приносните моменти са свързани с оценка и анализ на подходите за интеграция и конвергенция при киберсигурността, при което са разгледани следните въпроси: Специфика на тясно специализирани системи за откриване и реагиране на заплахи (TDR, EDR, NDR, XDR, MDR и CDR); Специфика на комплексни специализирани системи за откриване и реагиране на заплахи (SIEM, SOAR, SOC); Особености при развитието и съвместната работа на специализирани системи за откриване и реагиране на заплахи с други специализирани системи (CWPP, XSIAM и др.).

ИЗПОЛЗВАНИ ИЗТОЧНИЦИ REFERENCES

- [1] ПЕТРОВ, Георги. *Развитие на Интернет и отворените системи*. Ч. 1. София: Авангард Прима, 2017. ISBN 978-619-160-834-8. [PETROV, Georgi. *Razvitie na Internet i otvorenite sistemi*. Ch. 1. Sofia: Avangard Prima, 2017. ISBN 978-619-160-834-8.]
- [2] ПАСАРЕЛСКИ, Росен и Тереза СТЕФАНОВА. Методи за преход и внедряване на IPv6. *Управление и образование* [онлайн]. 2012, год. VIII (4), с. 203-211 [прегледан 20.03.2025]. ISSN 1312-6121. Достъпен на: https://www.conference-burgas.com/maevolumes/vol8/BOOK%204/b4_31.pdf [PASARELSKI, Rosen i Tereza STEFANOVA. Metodi za prehod i vnedryavane na IPv6. *Upravlenie i obrazovanie* [onlayn]. 2012, god. VIII (4), s. 203-211 [pregledan 20.03.2025]. ISSN 1312-6121. Dostapen na: https://www.conference-burgas.com/maevolumes/vol8/BOOK%204/b4_31.pdf]
- [3] ПАСАРЕЛСКИ, Росен и Теодора ПАСАРЕЛСКА. Виртуализация и сигурност в петото поколение 5G мобилни клетъчни мрежи. *Сборник статии от научна конференция „Знание, Наука, Иновации, Технологии“* [онлайн]. 2023, год. 2(1), с. 374-387 [прегледан 03.06.2026]. ISSN 2815-3480 . CEEOL. Достъпен на: <https://www.ceeol.com/> [PASARELSKI, Rosen i Teodora PASARELSKA. Virtualizatsia i sigurnost v petoto pokolenie 5G mobilni kletachni mrezhi. *Sbornik statii ot nauchna konferentsia „Znanie, Nauka, Inovatsii, Tehnologii“* [onlayn]. 2023, god. 2(1), s. 374-387 [pregledan 03.06.2026]. ISSN 2815-3480 . CEEOL. Dostapen na: <https://www.ceeol.com/>]
- [4] ПАСАРЕЛСКИ, Росен и Теодора ПАСАРЕЛСКА. Изследване на мрежовите функции и референтната архитектура на 5G мобилни системи. *Сборник статии от научна конференция „Знание, Наука, Иновации, Технологии“* [онлайн]. 2023, год. 2(1), с. 388-400 [прегледан 03.06.2026]. ISSN 2815-3480 . CEEOL. Достъпен на: <https://www.ceeol.com/> [PASARELSKI, Rosen i Teodora PASARELSKA. Izsledvane na mrezhovite funktzii i referentnata arhitektura na 5G mobilni sistemi. *Sbornik statii ot nauchna konferentsia „Znanie, Nauka, Inovatsii, Tehnologii“* [onlayn]. 2023, god. 2(1), s. 388-400 [pregledan 03.06.2026]. ISSN 2815-3480 . CEEOL. Dostapen na: <https://www.ceeol.com/>]
- [5] MILOVANOV, Nikolay. Case study: LoRa/LoRaWAN as a suitable LPWAN choice for pressure and flow monitoring in Bulgarian water utility sector. In: *CompSysTech '24: International Conference on Computer Systems and Technologies* [online]. 2024, pp. 173-179 [viewed 20.06.2026]. ISBN 979-8-4007-1684-3. Available from: <https://doi.org/10.1145/3674912.3674945>
- [6] ИВАНОВА, Йоана. Методи и средства за агентно-базирана визуализация на дигитализирани данни. *Годишник Телекомуникации* [онлайн]. 2021, Т. 8, с. 13-22 [прегледан 20.06.2026]. eISSN 2534-854X. Достъпен на: <https://doi.org/10.33919/YTelecomm.21.8.2> [IVANOVA, Yoana. Metodi i sredstva za agentno-bazirana vizualizatsia na digitalizirani dannii. *Godishnik Telekomunikatsii* [onlayn]. 2021, T. 8, s. 13-22 [pregledan 20.06.2026]. eISSN 2534-854X. Dostapen na: <https://doi.org/10.33919/YTelecomm.21.8.2>]
- [7] FIELDER, Christopher. Understanding the Lines Between EDR, NDR, TDR, XDR, and MDR. *Arctic Wolf* [online]. December 27, 2023 [viewed 20.03.2025]. Available from: <https://arcticwolf.com/resources/blog/understanding-between-edr-ndr-tdr-xdr-mdr/>
- [8] EDR vs NDR vs XDR vs MDR. *StreamSca* [online]. 30 june 2022 [viewed 20.03.2025]. Available from: <https://streamscan.ai/en/blog/edr-ndr-xdr-mdr/>
- [9] SIEM vs XDR vs SOAR vs SOC vs EDR vs MDR. *Blumira* [online]. December 12, 2023 [viewed 20.03.2025]. Available from: <https://www.blumira.com/blog/siem-soc-soar-xdr-defined>
- [10] What Is Cloud Detection and Response (CDR). *Paloalto* [online]. [viewed 20.03.2025]. Available from: <https://www.paloaltonetworks.com/cyberpedia/what-is-cloud-detection-and-response-cdr>

Информация за автора:

**ПЕРСПЕКТИВНИ СПЕЦИАЛИЗИРАНИ СИСТЕМИ ЗА ОТКРИВАНЕ И РЕАГИРАНЕ НА
ЗАПЛАХИ В КИБЕРСИГУРНОСТТА
ЦВЕТЕЛИНА СИМЕОНОВА**

гл. ас. д-р инж. Цветелина Симеонова, НБУ, департамент "Телекомуникации", ул. Монтевидео № 21, Тел.: 02 8110609, tsvsimeonova@nbu.bg

Contacts:

Chief Assist. Prof. Tsvetelina Simeonova, PhD, New Bulgarian University, Department "Telecommunications",
Tel.: 02 8110609, e-mail: tsvsimeonova@nbu.bg

Дата на постъпване на ръкописа (Date of receipt of the manuscript): 10.10.2024

Дата на приемане за публикуване (Date of adoption for publication): 30.09.2025