

Технічне завдання на придбання системи класу Decerption

Версія 2.0.
Дата 24.09.2026

Київ
2026

1. ТЕХНІЧНІ ВИМОГИ

1.1.	Клас системи	Deception
1.2.	Призначення системи	Виявлення дій атакуючих, при їх проникненні в периметр мережі, за рахунок створення пасток та емуляції елементів IT та OT інфраструктури Групи Метінвест.
1.3.	Загальний опис	Система повинна забезпечувати створення та/або розгортання об'єктів-приманок (decoys, honeypots, deception assets) у корпоративній IT-інфраструктурі з метою виявлення несанкціонованої розвідки, спроб доступу, горизонтального поширення та інших несанкціонованих дій потенційного зломисника
Вимоги суворой відповідності		
1.4.	Вимоги до виробника	Перелік виробників рішень що розглядаються: • Acalvio ShadowPlex • Fortinet FortiDeceptor • Proofpoint Illusive • SentinelOne Attivo • Thinkst Canary • Fidelis Deception • Commvault ThreatWise • Rapid7 Deception • TrapX Security • CounterCraft • Labyrinth Cyber Deception Platform • Tracebit • ПЗ інших вендорів класу Deception за умови відповідності Технічному завданню
1.5.	Функціональні вимоги до системи	1.5.1. Система має включати централізований інтерфейс\сервер керування своїми компонентами/ 1.5.2. Система повинна підтримувати емуляцію або імітацію мережеских вузлів та/або сервісів щонайменше таких функціональних категорій: - серверні та/або клієнтські системи; - мережескі сервіси; - файлові ресурси; - web-сервіси; - сервіси автентифікації та/або каталогів; - бази даних або сервіси доступу до баз даних тощо. 1.5.3. Система повинна підтримувати створення та/або розміщення одного або декількох типів deception-артефактів у продуктивному середовищі, зокрема: - облікових записів-приманок; - фіктивних credentials; - файлів та документів-приманок; - посилань на мережескі ресурси; - мережеских або прикладних сервісів; - інших honeytokens/breadcrumbs/lures.

		1.5.4. Система повинна забезпечувати виявлення взаємодії користувача, процесу, пристрою або мережевого вузла з об'єктом чи артефактом-приманкою та формувати відповідну подію/сповіщення інформаційної безпеки та передавати її до SIEM Microsoft Sentinel 1.5.5. Система повинна забезпечувати можливість виявлення ознак несанкціонованого горизонтального поширення у корпоративній інфраструктурі шляхом використання об'єктів та/або артефактів-приманок. Можуть використовуватися, залежно від архітектури рішення: decoy systems, deceptive credentials, honey accounts, honey files, breadcrumbs, network services, honeytokens або функціонально еквівалентні механізми. 1.5.6. Система повинна забезпечувати можливість використання фіктивних ідентифікаційних даних та/або інших deception-артефактів для виявлення спроб несанкціонованого використання облікових даних та доступу до інформаційних ресурсів 1.5.7. Система повинна забезпечувати розгортання deception-компонентів у декількох мережевих сегментах/VLAN без необхідності зміни логіки роботи продуктивних інформаційних систем 1.5.8. Система повинна забезпечувати можливість представлення об'єкта-приманки як мережевого ресурсу, доступного за IP-адресою та/або відповідними мережевими сервісами. 1.5.9. Взаємодія з об'єктом-приманкою повинна дозволяти визначити щонайменше: - час взаємодії; - IP-адресу джерела; - об'єкт/сервіс, з яким здійснювалася взаємодія; - тип події; - додаткову інформацію про взаємодію, якщо вона доступна відповідно до архітектури системи. 1.5.10. Система повинна забезпечувати централізований перегляд подій/сповіщень, сформованих у результаті взаємодії з deception-об'єктами
1.6.	Вимоги по доступу до системи	Система має підтримувати рольове розмежування доступу та включати наступні ролі (можуть називатися інакше, але містити відповідний функціонал): - Адміністратор – має повний доступ до системи та має право створювати пастки - Аналітик з інцидентів – має право переглядати та закривати події, виявлені системою.
1.7.	Вимоги щодо ліцензування	Система має дозволяти перепризначати ліцензію.
1.8.	Вимоги до сайзингу системи	Система має забезпечити розміщення: - до 500 мережевих пасток, які мають бути доступними для підключення з будь якої мережі Групи за умови наявності маршрутизації та правил мережевої взаємодії. - в 90 VLAN в яких розміщено 3000 корпоративних пристроїв - з використанням до 30 віртуальних апласнів в приватних датацентрах Групи

2. ВИМОГИ ДО ВПРОВАДЖЕННЯ (якщо ПЗ не Commvault ThreatWise)

2.1.	Архітектура	Виконавець спільно з замовником розробляє архітектуру рішення в термін до 1 місяця після заключення Договору. В рамках розробки архітектури мають бути затверджені: - системні вимоги до системи - детальна архітектура системи - кількість та розміщення компонент системи в дата центрах Групи - IP план пасток що включає: IP адресу, маску підмережі, VLAN ID, тип пастки, назву пастки, прив'язку до аплаєнсу																																							
2.2.	Установка системи	Виконавець виконує встановлення та налаштування системи протягом 1 місяця з дати надання необхідних ресурсів (створення віртуальних серверів згідно затвердженої архітектури). Перелік датацентрів та аплаєнсів для встановлення та налаштування: <table><tr><td></td><td>MTM</td><td>FVS</td><td>SPT</td><td>PMS</td><td>DMK</td><td>CGK</td><td>IGK</td><td>SGK</td><td>ZST</td><td>Azure</td><td>Adria</td><td>IASV</td></tr><tr><td>Пастки</td><td>56</td><td>36</td><td>59</td><td>17</td><td>72</td><td>36</td><td>35</td><td>47</td><td>45</td><td>50</td><td>22</td><td>22</td></tr><tr><td>Аплаєнси</td><td>2</td><td>1</td><td>2</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>3</td><td>3</td><td>1</td><td>1</td></tr></table> Кожна пастка має бути протестована на коректність спрацювання. Виконавець налаштовує автоматичне оновлення компонент системи. Виконавець налаштовує надані Замовником виключення, відомі на момент впровадження системи. Виконавець налаштовує рольову модель доступу до системи.		MTM	FVS	SPT	PMS	DMK	CGK	IGK	SGK	ZST	Azure	Adria	IASV	Пастки	56	36	59	17	72	36	35	47	45	50	22	22	Аплаєнси	2	1	2	1	2	2	2	2	3	3	1	1
	MTM	FVS	SPT	PMS	DMK	CGK	IGK	SGK	ZST	Azure	Adria	IASV																													
Пастки	56	36	59	17	72	36	35	47	45	50	22	22																													
Аплаєнси	2	1	2	1	2	2	2	2	3	3	1	1																													
2.3.	Створення інтеграцій	Виконавець виконує інтеграції: 1. З корпоративною системою централізованої авторизації Замовника 2. З SIEM системою замовника (Microsoft Sentinel).																																							
2.4.	Розробка документації	Виконавець має створити а Замовник перевірити та затвердити наступний перелік документації (допускається використання інформації від вендора Системи): - Інструкція адміністратора із зазначенням дій щодо налаштування компонент системи, оновлення, моніторингу стану та первинної діагностики компонент системи, створення пасток, внесення виключень.																																							
2.5.	Прийняття системи в експлуатацію	Виконавець узгоджує з замовником методику прийняття системи в експлуатацію, обов'язкові етапи: - Перевірка функціоналу системи - Перевірка роботи інтеграцій - Перевірка технічної документації																																							
2.6.	Технічна підтримка	Виконавець має передати замовнику контакти технічної підтримки.																																							
2.7.	Навчання	Виконавець проводить навчання по роботі в системі представників Замовника. Навчання має включати та не обмежуватись такими темами: налаштування компонент системи, оновлення, моніторингу стану та первинної діагностики компонент системи, створення пасток, внесення виключень.																																							

3. ВИМОГИ ОЦІНКИ

Вимоги суворой відповідності	
Пропозиції, які не відповідають вимогам суворой відповідності відхиляються. Відповідність вимогам має бути підтверджена через надання документації виробника або шляхом демонстрації функціонала.	
Відповідність вимогам, зазначеним в пунктах 1 та 2.	
Виконавець має статус партнера виробника системи що впроваджується	
Виконавець має досвід успішного впровадження системи в промислову експлуатацію у одного та більше замовників	

4. КВАЛІФІКАЦІЙНА ЧАСТИНА

Компанія-претендент надає:

- Інформацію про партнерські відносини з вендором рішення.
- Інформацію про досвід та відгуки замовників (100+ співробітників) щодо аналогічних впроваджень.
- Сертифікати фахівців та інші профільні у сфері інформаційної безпеки.
- Підтвердження відповідності вимогам суворой відповідності у вигляді посилань на технічну документацію виробника.
- Проводить демонстрацію відповідності вимогам суворой відповідності на власному стенді.

Компанія-претендент підтверджує:

- Реєстрацію компанії не пізніше 2022 року (компанія на ринку України не менше 3 років) з наданням документів про реєстрацію компанії.