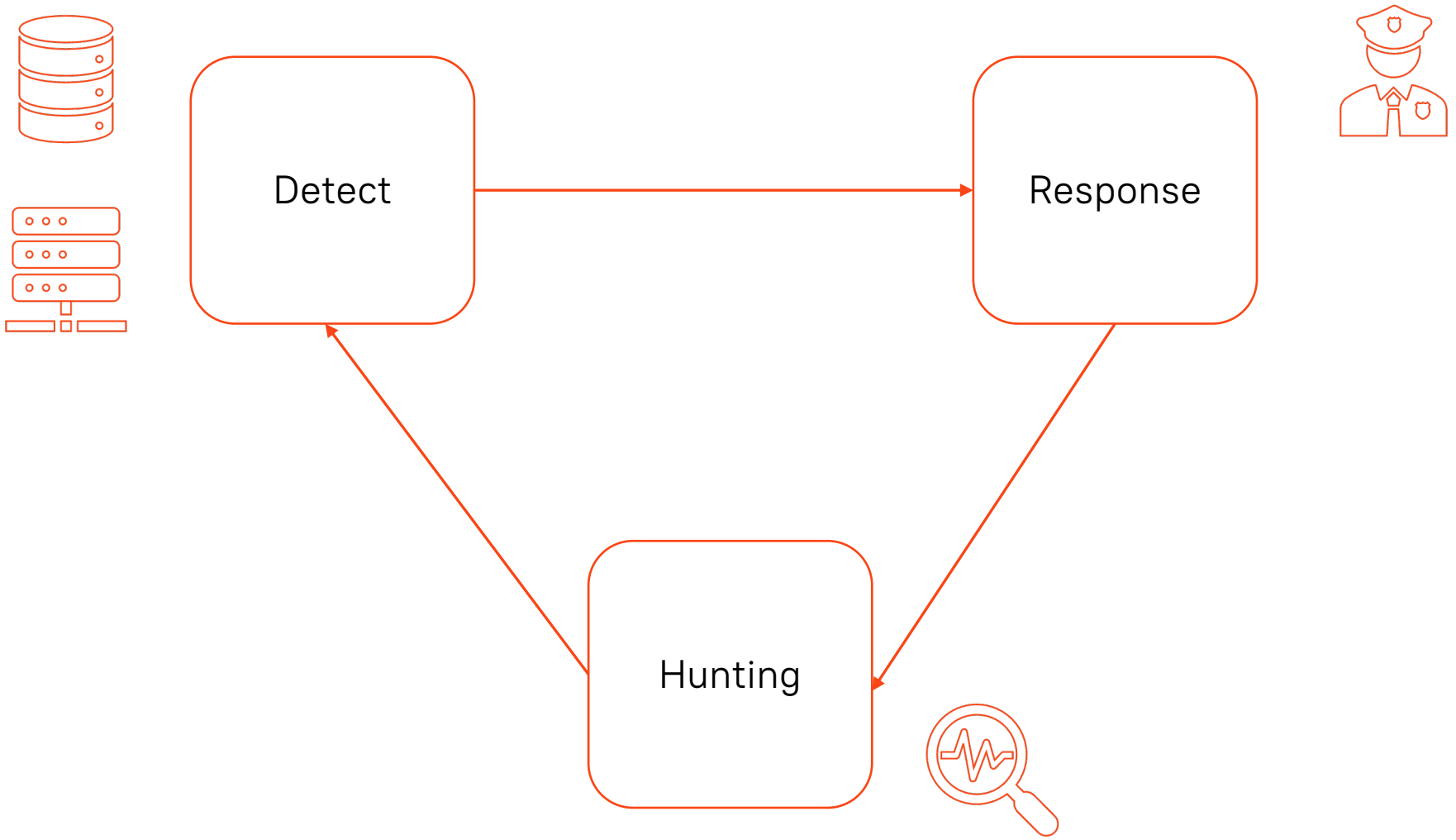
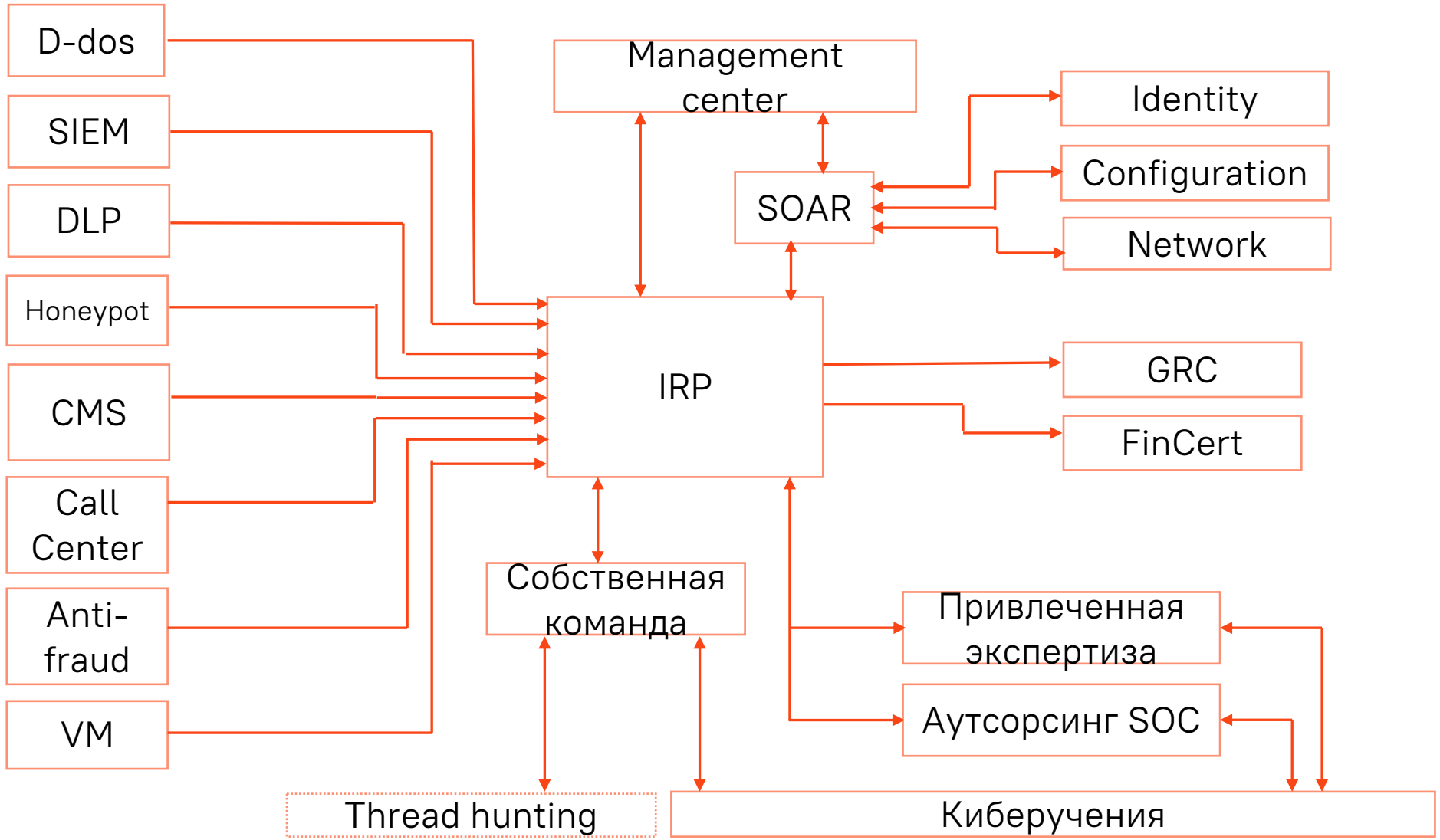
SOC на примере Абсолютбанк

абсолют банк

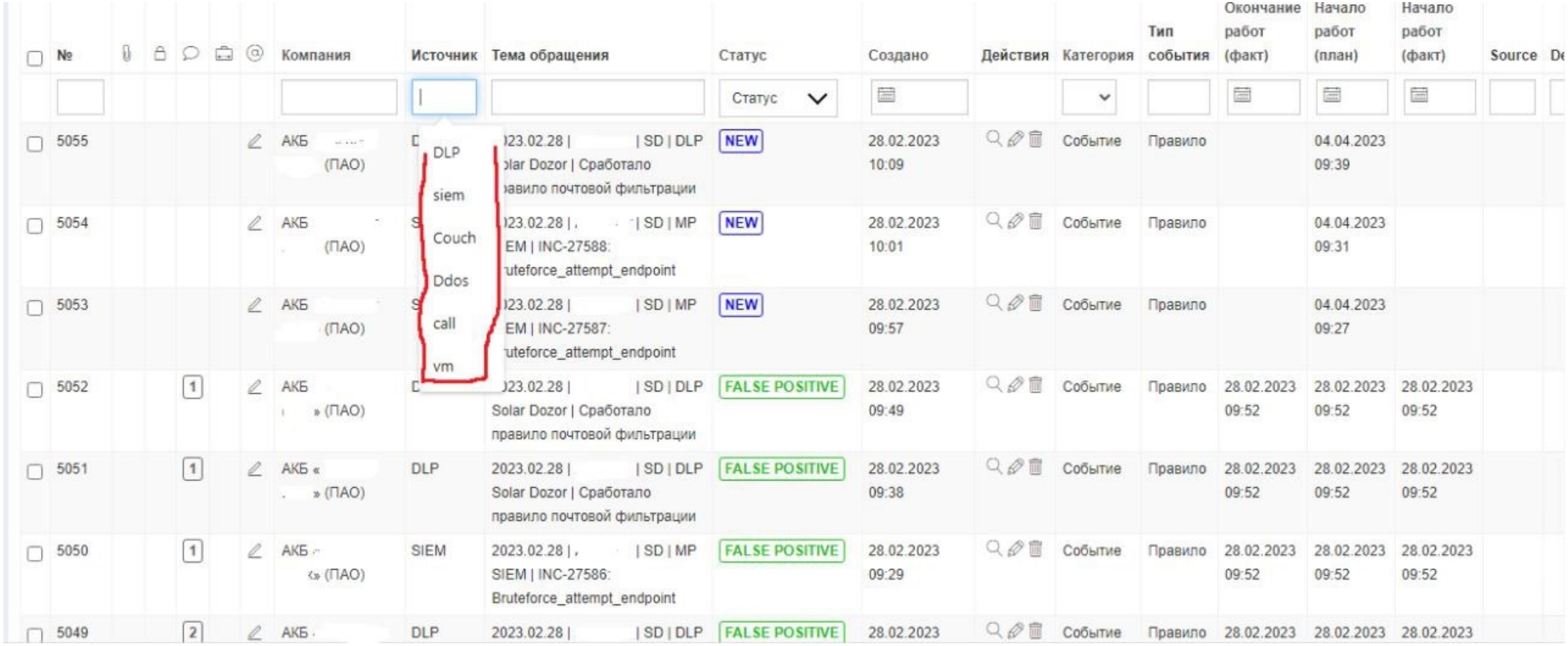
Управление инцидентами



Гибридный SOC



Источники событий

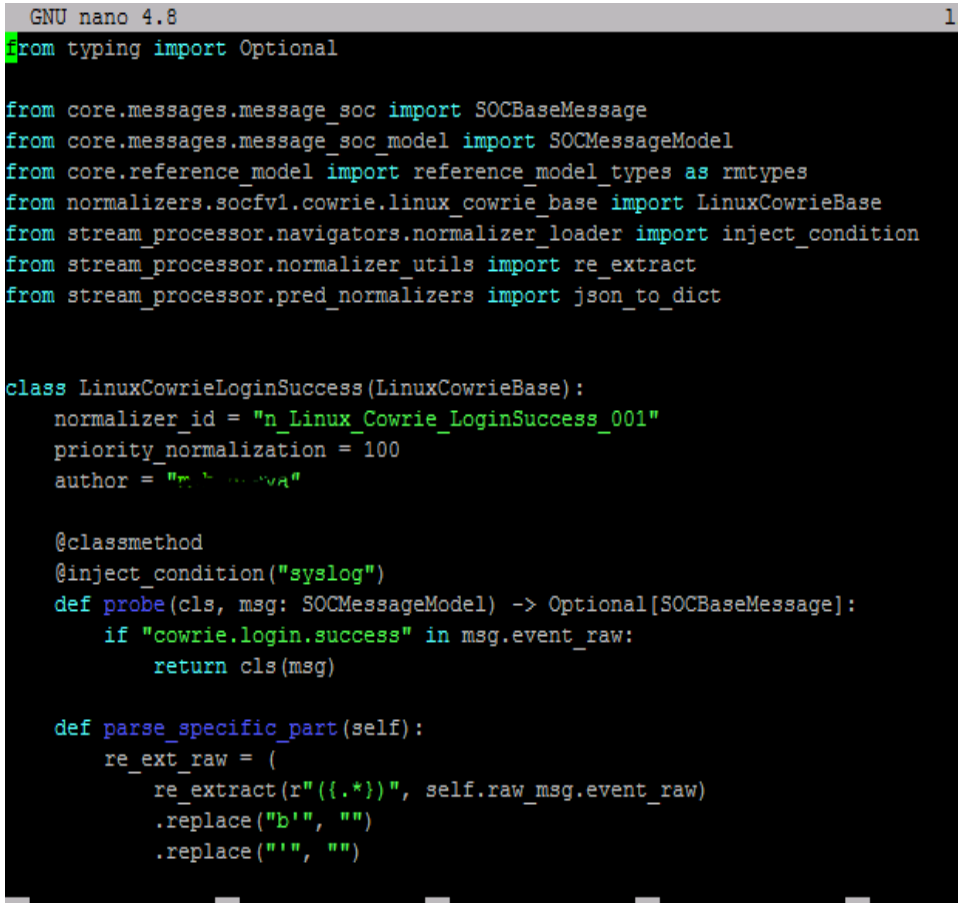


№	Компания	Источник	Тема обращения	Статус	Создано	Действия	Категория	Тип события	Окончание работ (факт)	Начало работ (план)	Начало работ (факт)	Source
5055	АКБ (ПАО)	D	023.02.28 | | SD | DLP olar Dozor | Сработало авило почтовой фильтрации	NEW	28.02.2023 10:09		Событие	Правило		04.04.2023 09:39		
5054	АКБ (ПАО)	S	023.02.28 | , | SD | MP EM | INC-27588: uteforce_attempt_endpoint	NEW	28.02.2023 10:01		Событие	Правило		04.04.2023 09:31		
5053	АКБ (ПАО)	S	023.02.28 | | SD | MP EM | INC-27587: uteforce_attempt_endpoint	NEW	28.02.2023 09:57		Событие	Правило		04.04.2023 09:27		
5052	АКБ » (ПАО)	D	023.02.28 | | SD | DLP Solar Dozor | Сработало правило почтовой фильтрации	FALSE POSITIVE	28.02.2023 09:49		Событие	Правило	28.02.2023 09:52	28.02.2023 09:52	28.02.2023 09:52	
5051	АКБ « » (ПАО)	DLP	2023.02.28 | | SD | DLP Solar Dozor | Сработало правило почтовой фильтрации	FALSE POSITIVE	28.02.2023 09:38		Событие	Правило	28.02.2023 09:52	28.02.2023 09:52	28.02.2023 09:52	
5050	АКБ » (ПАО)	SIEM	2023.02.28 | , | SD | MP SIEM | INC-27586: Bruteforce_attempt_endpoint	FALSE POSITIVE	28.02.2023 09:29		Событие	Правило	28.02.2023 09:52	28.02.2023 09:52	28.02.2023 09:52	
5049	АКБ	DLP	2023.02.28 | | SD | DLP	FALSE POSITIVE	28.02.2023		Событие	Правило	28.02.2023	28.02.2023	28.02.2023	

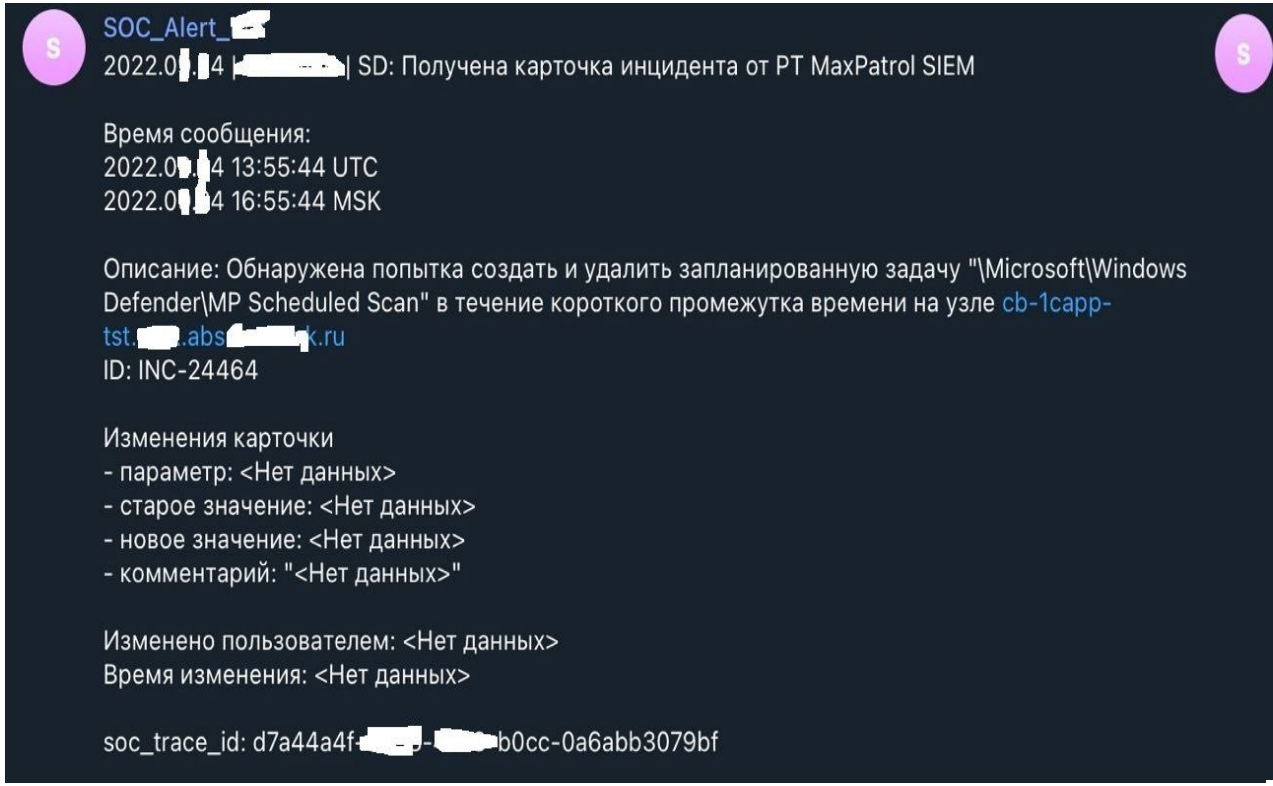
Индикаторы активностей

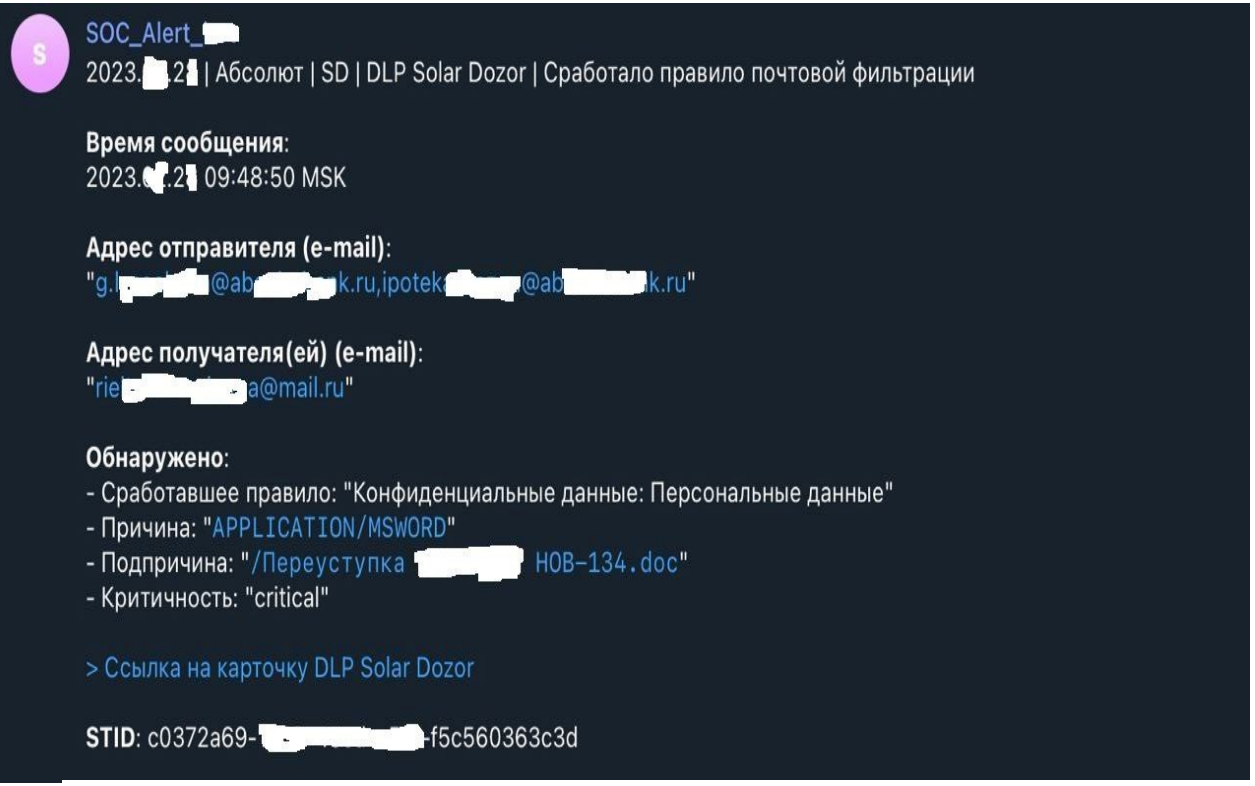
Обогащение события

- Перебор пароля учётной записи (УЗ) на устройстве доступа
- Подключение к ханипоту
- Срабатывание правил DLP
- Запуск недоверенного ПО
- Очистка журнала безопасности Windows.



Расследование инцидентов





Спасибо

Ложкин Р.В.

E-mail: r.lozhkin@absolutbank.ru

абсолют банк