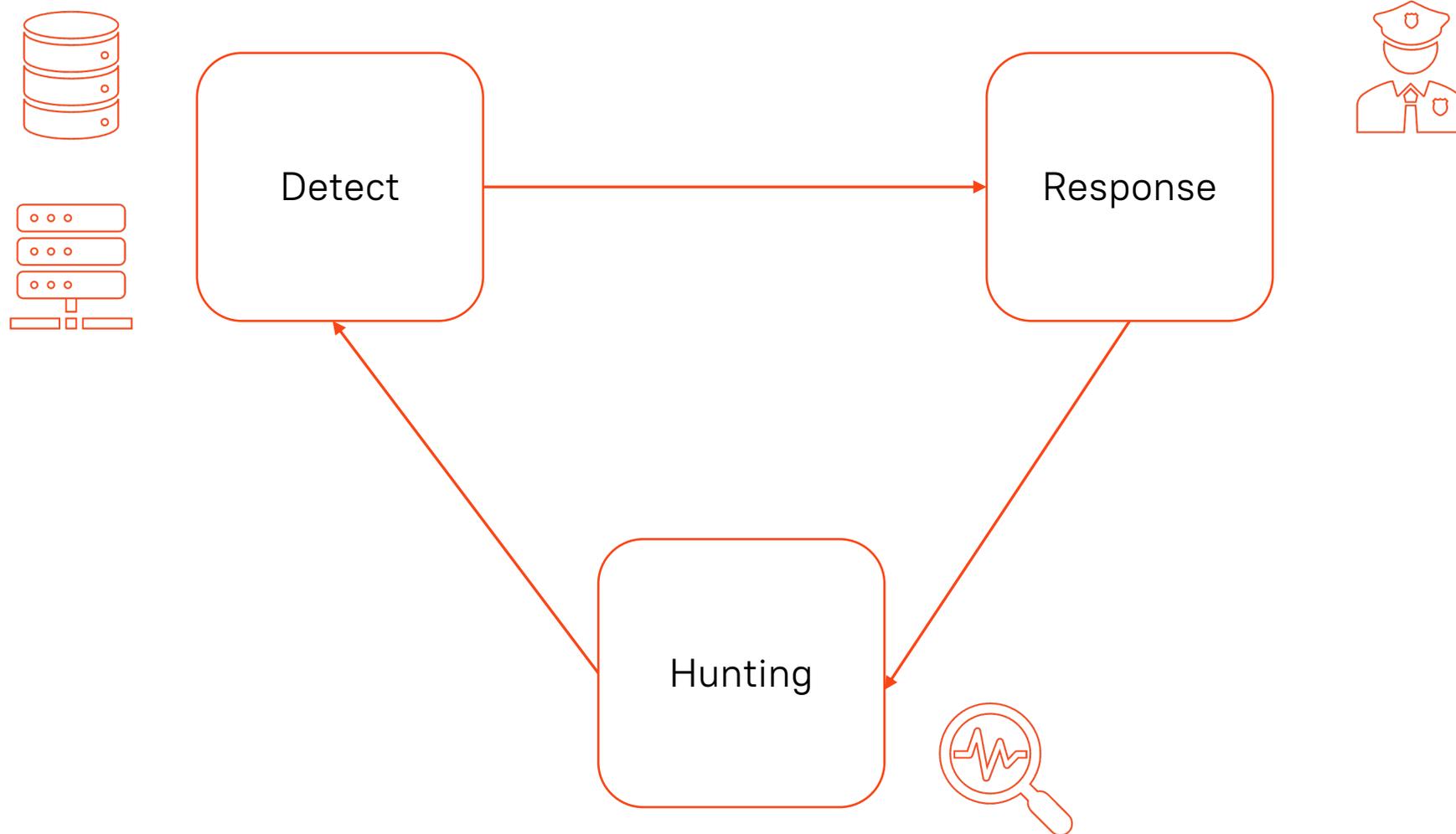




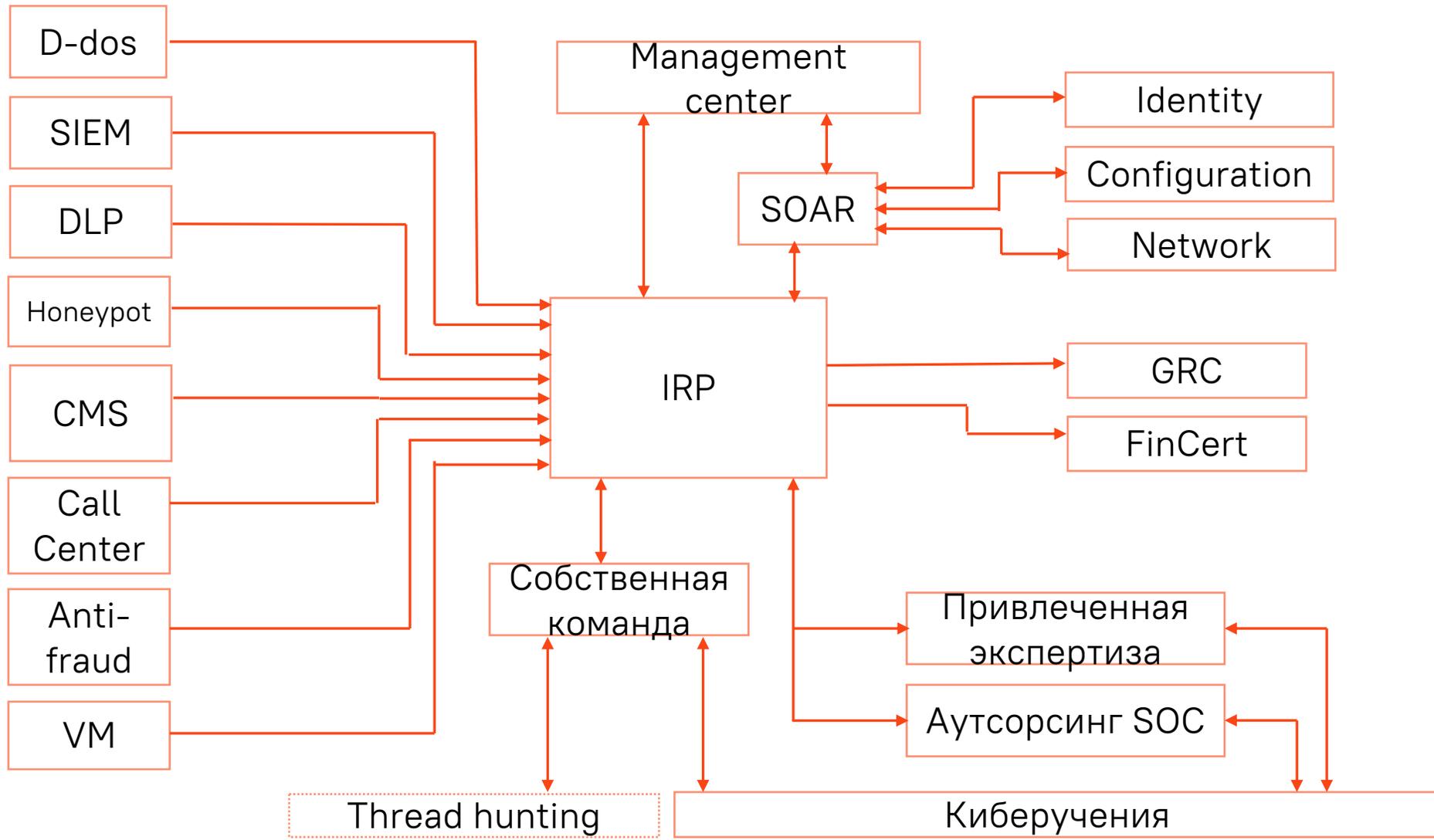
SOC на примере Абсолютбанк

**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	De
5055	АКБ «...» (ПАО)	DLP	23.02.28 SD DLP Solar Dozor Сработало правило почтовой фильтрации	NEW	28.02.2023 10:09	🔍 ✎ 🗑️	Событие	Правило		04.04.2023 09:39			
5054	АКБ «...» (ПАО)	SIEM Couch	23.02.28 SD MP EM INC-27588: bruteforce_attempt_endpoint	NEW	28.02.2023 10:01	🔍 ✎ 🗑️	Событие	Правило		04.04.2023 09:31			
5053	АКБ «...» (ПАО)	SIEM Ddos	23.02.28 SD MP EM INC-27587: bruteforce_attempt_endpoint	NEW	28.02.2023 09:57	🔍 ✎ 🗑️	Событие	Правило		04.04.2023 09:27			
5052	АКБ «...» (ПАО)	DLP	23.02.28 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 «...» (ПАО)	DLP	2023.02.28 SD DLP	FALSE POSITIVE	28.02.2023	🔍 ✎ 🗑️	Событие	Правило	28.02.2023	28.02.2023	28.02.2023		

Индикаторы активностей

	Утилизация канала		
DDOS	0%		
Сканировані периметра	0		
Уязвимости периметра	0	0	0
Атака на периметр	0		
Уязвимости WEB	0	0	0
Атака на WEB	0		

	Servers	Desktop	ATM
Вредоносное ПО	1	0	0
Брутфорс	15		
Подозрительная активность	0		
Обход СЗИ	0		
Уязвимости VM	HIGH 0	AVG 0	LOW 0
Уязвимости Couch	HIGH 0	AVG 0	LOW 0

Обогащение события

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

```
GNU nano 4.8 1
from typing import Optional

from core.messages.message_soc import SOCBaseMessage
from core.messages.message_soc_model import SOCMessageModel
from core.reference_model import reference_model_types as rmtypes
from normalizers.socfv1.cowrie.linux_cowrie_base import LinuxCowrieBase
from stream_processor.navigators.normalizer_loader import inject_condition
from stream_processor.normalizer_utils import re_extract
from stream_processor.pred_normalizers import json_to_dict

class LinuxCowrieLoginSuccess(LinuxCowrieBase):
    normalizer_id = "n_Linux_Cowrie_LoginSuccess_001"
    priority_normalization = 100
    author = "m. b. ...ova"

    @classmethod
    @inject_condition("syslog")
    def probe(cls, msg: SOCMessageModel) -> Optional[SOCBaseMessage]:
        if "cowrie.login.success" in msg.event_raw:
            return cls(msg)

    def parse_specific_part(self):
        re_ext_raw = (
            re_extract(r"({.*})", self.raw_msg.event_raw)
            .replace("b'", "")
            .replace("'", "")
```

Расследование инцидентов



SOC_Alert_

2022.01.14 | | SD: Получена карточка инцидента от PT MaxPatrol SIEM

Время сообщения:

2022.01.14 13:55:44 UTC

2022.01.14 16:55:44 MSK

Описание: Обнаружена попытка создать и удалить запланированную задачу "\Microsoft\Windows Defender\MP Scheduled Scan" в течение короткого промежутка времени на узле [cb-1capp-tst. abs. k.ru](#)

ID: INC-24464

Изменения карточки

- параметр: <Нет данных>
- старое значение: <Нет данных>
- новое значение: <Нет данных>
- комментарий: "<Нет данных>"

Изменено пользователем: <Нет данных>

Время изменения: <Нет данных>

soc_trace_id: d7a44a4f- - b0cc-0a6abb3079bf



SOC_Alert_

2023.01.21 | Абсолют | SD | DLP Solar Dozor | Сработало правило почтовой фильтрации

Время сообщения:

2023.01.21 09:48:50 MSK

Адрес отправителя (e-mail):

"g.l. @ab. k.ru,ipotek. @ab. k.ru"

Адрес получателя(ей) (e-mail):

"rie. @mail.ru"

Обнаружено:

- Сработавшее правило: "Конфиденциальные данные: Персональные данные"
- Причина: "APPLICATION/MSWORD"
- Подпричина: "/Переуступка. HOB-134.doc"
- Критичность: "critical"

> [Ссылка на карточку DLP Solar Dozor](#)

STID: c0372a69- - f5c560363c3d

Спасибо

Ложкин Р.В.

E-mail: r.lozhkin@absolutbank.ru

АБСОЛЮТ
БАНК