



POSITIVE
TECHNOLOGIES

Threat hunting: поиск угроз, когда системы ИБ молчат

Антон Тюрин

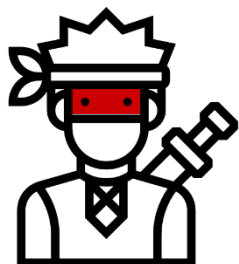
Руководитель отдела экспертных сервисов PT ESC



WHOAMI

PT

ptsecurity.com/ru-ru/services/esc/



- Работаю в PT Expert Security Center
- Отвечаю за обнаружение атак в сети и на хосте
- Разрабатываю правила и корреляции
- Провожу threat hunting в инфраструктуре заказчика

5000 правил

Партнёрство с any.run

Публикации в наборе от ET Open и Cisco Talos

Threat hunting



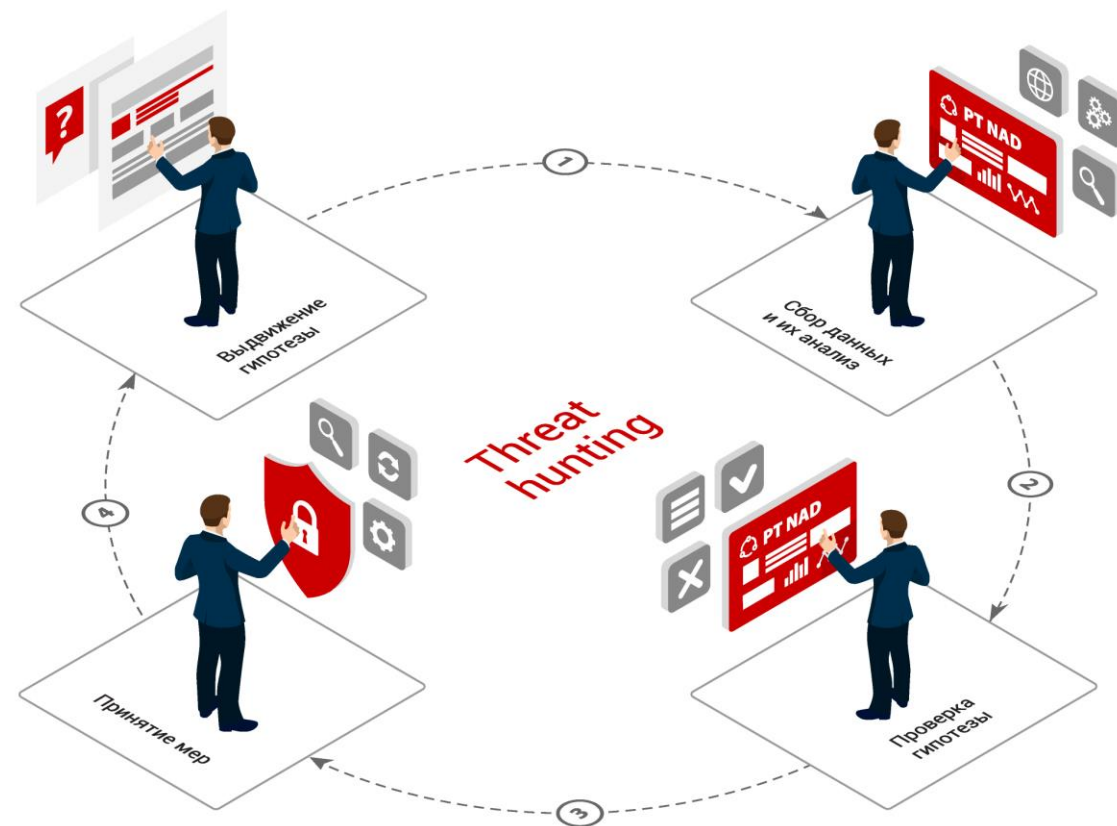
Процесс проактивного поиска угроз в сети, которые не обнаруживаются традиционными средствами безопасности

Помогает:

- Выявить существующую компрометацию
- Найти уязвимые места в инфраструктуре до возникновения инцидента

Что нужно:

- Системы сбора и анализа данных
- Гипотеза



Источники идей для гипотез:

MITRE ATT&CK

База знаний, основанная на анализе реальных АРТ-атак. Описывает распространенные тактики и техники атак: attack.mitre.org/

Threat intelligence

Экспертиза вендоров об актуальных видах угроз и трендах атак.

Аналитика по пентестам

Исследования векторов проникновения в сеть.
Пример: [Уязвимости корпоративных информационных систем](#), Positive Technologies, 2019.

Знание инфраструктуры

Знание слабых мест своей инфраструктуры и предположения о том, как их могут проэксплуатировать злоумышленники.

He threat hunting:

PT

- × Реагирование на алерт в системе ИБ

PT Network Attack Discovery —

система глубокого анализа
сетевого трафика (NTA)
для выявления атак
на периметре и внутри сети

**NTA – network traffic analysis*

- **Дает понимание,
что происходит в сети**
Определяет 50 протоколов,
30 разбирает на уровнях L2-L7
- **Выявляет атаки в реальном
времени и в ретроспективе**
Пополнение базы знаний
2 раза в неделю
- **Помогает в расследованиях
и threat hunting**
Хранит сырой трафик
и 1200 параметров сессий





Кейс №1

ptsecurity.com

Houston, we have an intruder



Гипотеза: в инфраструктуре есть бэкдор и он отстукивается наружу.

Что потребуется: анализ соединений во вне, анализ пейлоадов.



Кейс №2

ptsecurity.com

Аномалии в LDAP-запросах

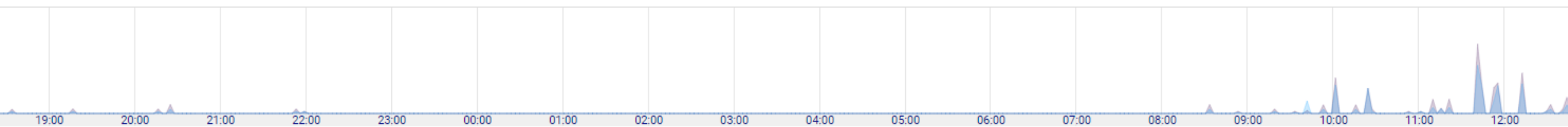


Гипотеза: инфраструктура скомпрометирована, и атакующие находятся на стадии Lateral Movement. Без разведки внутри Active Directory это не обойдется.

Что потребуется: анализ соединений внутри сети, разбор LDAP-трафика, знание о профиле легитимных запросов.

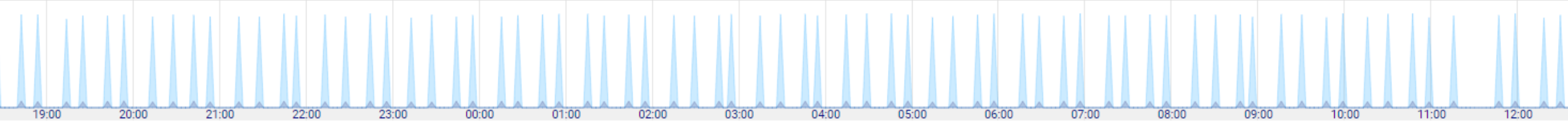
← → app_proto == 'ldap' && ldap.rqs.search.filter ~ '*mail=*'

Общий трафик 1.95 МБ: ■ отправлено 1.19 МБ ■ получено 759.96 кБ Средняя скорость трафика 23 Б/с



```
"search": {
  "attributes": [
    "objectCategory",
    "msExchRecipientDisplayType",
    "distinguishedName",
    "msRTCSIP-PrimaryUserAddress",
    "mail",
    "displayName",
    "title",
    "company",
    "department",
    "physicalDeliveryOfficeName",
    "telephoneNumber",
    "mobile",
    "homePhone",
    "manager",
    "description",
    "postalCode",
    "streetAddress",
    "st",
    "l",
    "c",
    "wwwHomePage",
    "givenName",
    "sn"
  ],
  "base_object": "",
  "deref_aliases": "never deref aliases",
  "filter": "(&(|(mail=*@*.com)(proxyAddresses=smtp:*.com)))",
  "scope": "whole_subtree",
  "size_limit": 1000,
  "time_limit": 60,
  "types_only": false
},
"type": "search"
```


Общий трафик 43.19 МБ: ■ отправлено 2.74 МБ ■ получено 40.45 МБ Средняя скорость трафика 506 Б/с



```
{
  "msExchUMPhoneContext": {
    "base_object": "CN=Configuration,DC=example.com",
    "deref_aliases": "never_deref_aliases",
    "filter": "(&(objectCategory=msExchUMDialPlan)(msExchUMDialPlanURIType=3))",
    "scope": "whole_subtree",
    "size_limit": 0,
    "time_limit": 0,
    "types_only": false
  },
  "type": "search"
},
{
  "rsp": {
    "diag_msg": "",
    "entries": [
      {
        "attributes": [
          {
            "type": "name",
            "vals": [
              ""
            ]
          },
          {
            "type": "msExchUMPhoneContext",
            "vals": [
              ""
            ]
          }
        ],
        "type": "msExchUMServerDialPlanBL",
        "vals": [
          "CN=UMCallRouterSettings,CN=SIP,CN=Protocols,CN=Example.com,CN=Servers,CN=Exchange Administrative Group",
          "CN=Admini..."
        ]
      }
    ]
  }
}
```

Kerberoasting

Запрос
учетных
записей с
**Service
Principal
Name (SPN)**

Запрос
Kerberos-
билетов (TGS)
для целевых
сервисных
аккаунтов

Экспорт
Kerberos-
билетов в
файлы

Взлом NTLM-
хешей
сервисных
аккаунтов на
стороне
атакующего

Получение
паролей
сервисных
аккаунтов в
открытом виде



Кейс №3

ptsecurity.com

От периметра к DC



Гипотеза: скомпрометирована учетка из группы Domain Admins, нелегитимные подключения к контроллеру домена.

Что потребуется: тяжелый труд.

Рецепт:

The logo consists of the letters 'PT' in a white, sans-serif font, centered within a gray square.

- Не ждать у моря алертов
- Знать свою инфраструктуру и техники атакующих, чтобы строить гипотезы
- Воспроизводить техники, чтобы знать, какие артефакты искать
- Threat hunting становится проще, когда есть много разложенных по полочкам данных и удобные инструменты для поиска

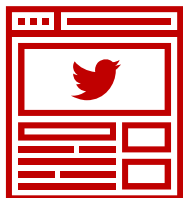
22.6%

организаций повысили
свой уровень
защищенности на 21-
30% благодаря
использованию Threat
hunting подхода

[SANS 2018 Threat Hunting Survey Results](#)

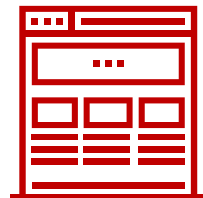
Полезные ссылки:

PT



Twitter

twitter.com/AttackDetection



Blog

habr.com/company/pt/blog/



**Threat Intelligence
отчеты и публикации**

ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/



**Пропилотировать
PT NAD:**

ptsecurity.com/ru-ru/products/network-attack-discovery/

Антон Тюрин

Руководитель отдела экспертных сервисов PT ESC

ATyurin@ptsecurity.com