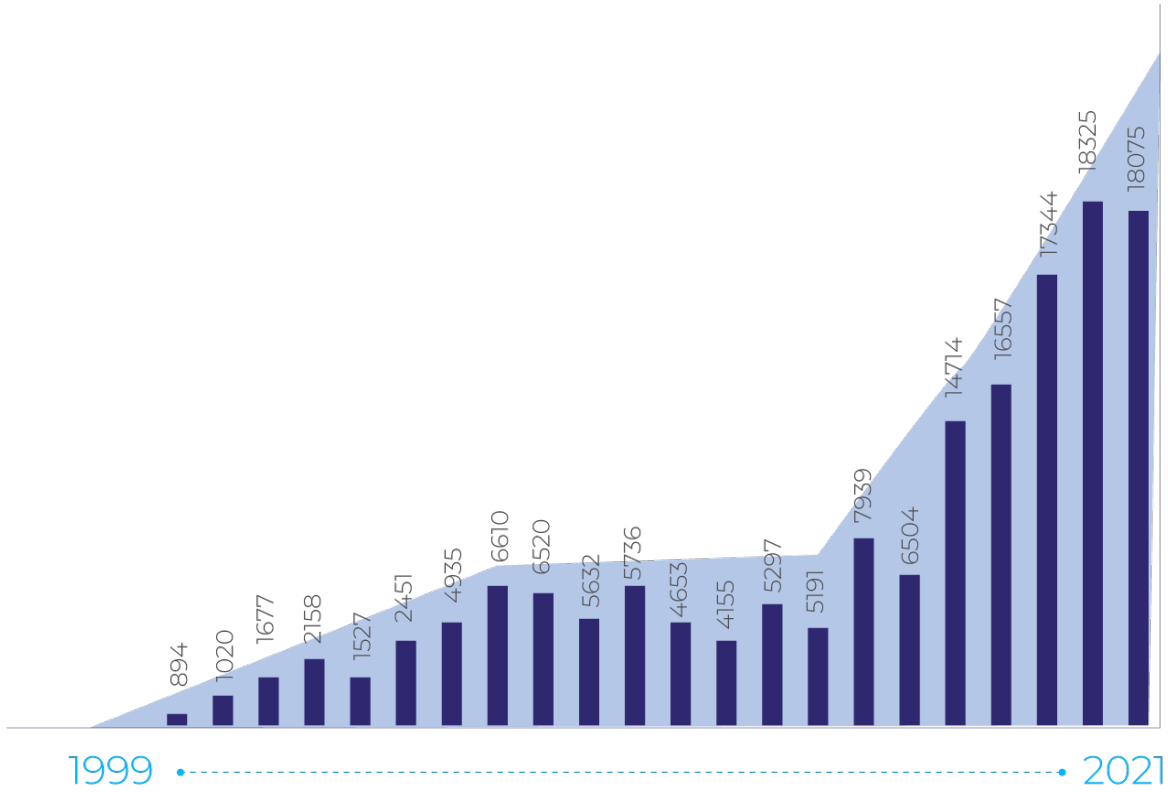
SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

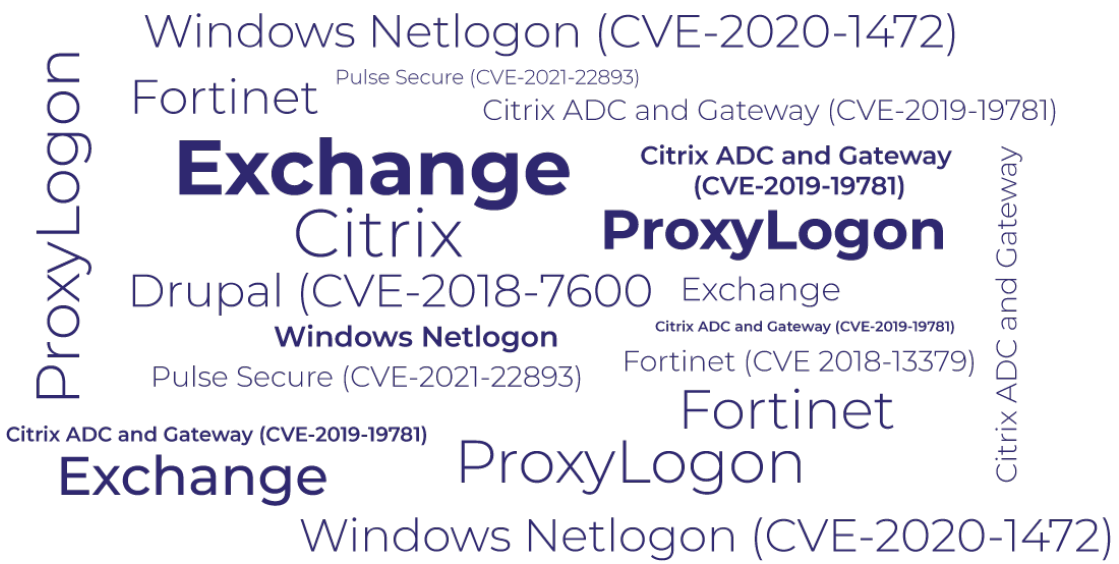
Видишь дыру?

Нет? А она есть!

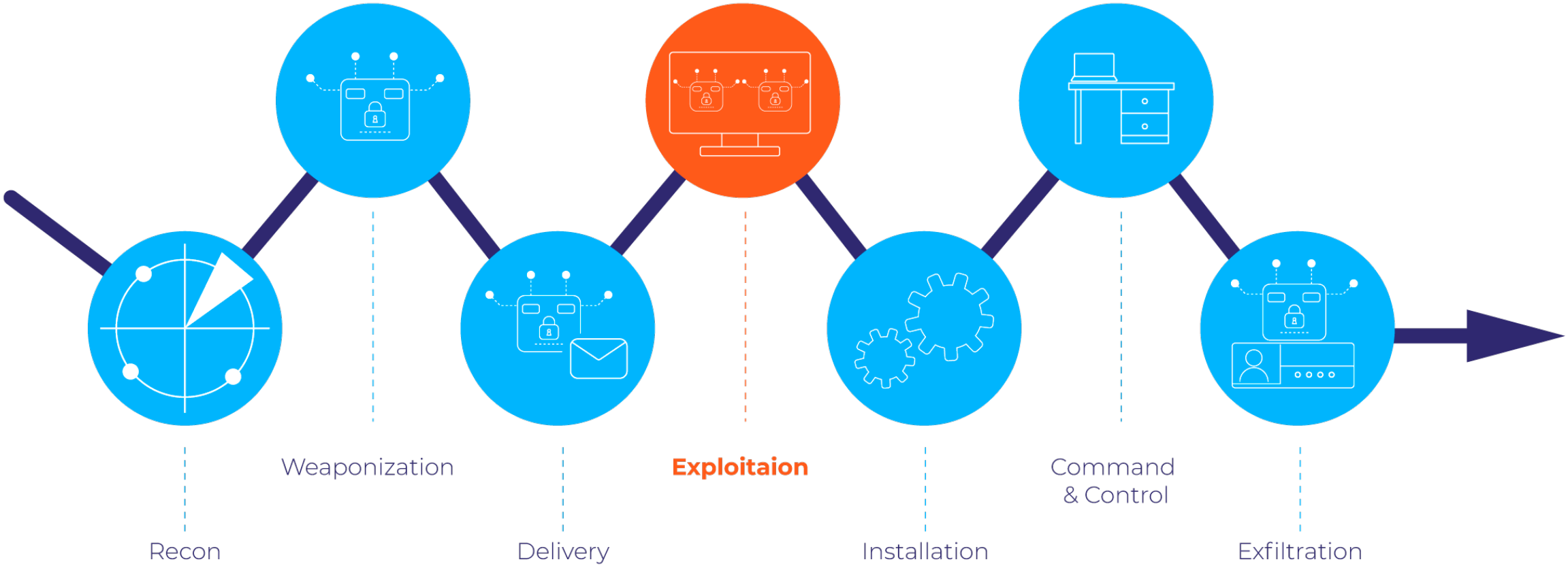
Роман Овчинников,
Руководитель отдела исполнения

Статистика


894
1020
1677
2158
1527
2451
4935
6610
6520
5632
5736
4653
4155
5297
5191
7939
6504
14714
16557
17344
18325
18075
1999
2021


Windows Netlogon (CVE-2020-1472)
ProxyLogon
Fortinet
Pulse Secure (CVE-2021-22893)
Citrix ADC and Gateway (CVE-2019-19781)
Exchange
Citrix ADC and Gateway (CVE-2019-19781)
Citrix
ProxyLogon
Drupal (CVE-2018-7600
Exchange
Citrix ADC and Gateway (CVE-2019-19781)
Windows Netlogon
Pulse Secure (CVE-2021-22893)
Fortinet (CVE 2018-13379)
Fortinet
Citrix ADC and Gateway (CVE-2019-19781)
Exchange
ProxyLogon
Citrix ADC and Gateway
Windows Netlogon (CVE-2020-1472)

Роль уязвимости



Применение в SOC

01 Реагирование на инциденты – повышение качества приоритезации, анализа, сдерживания и устранения

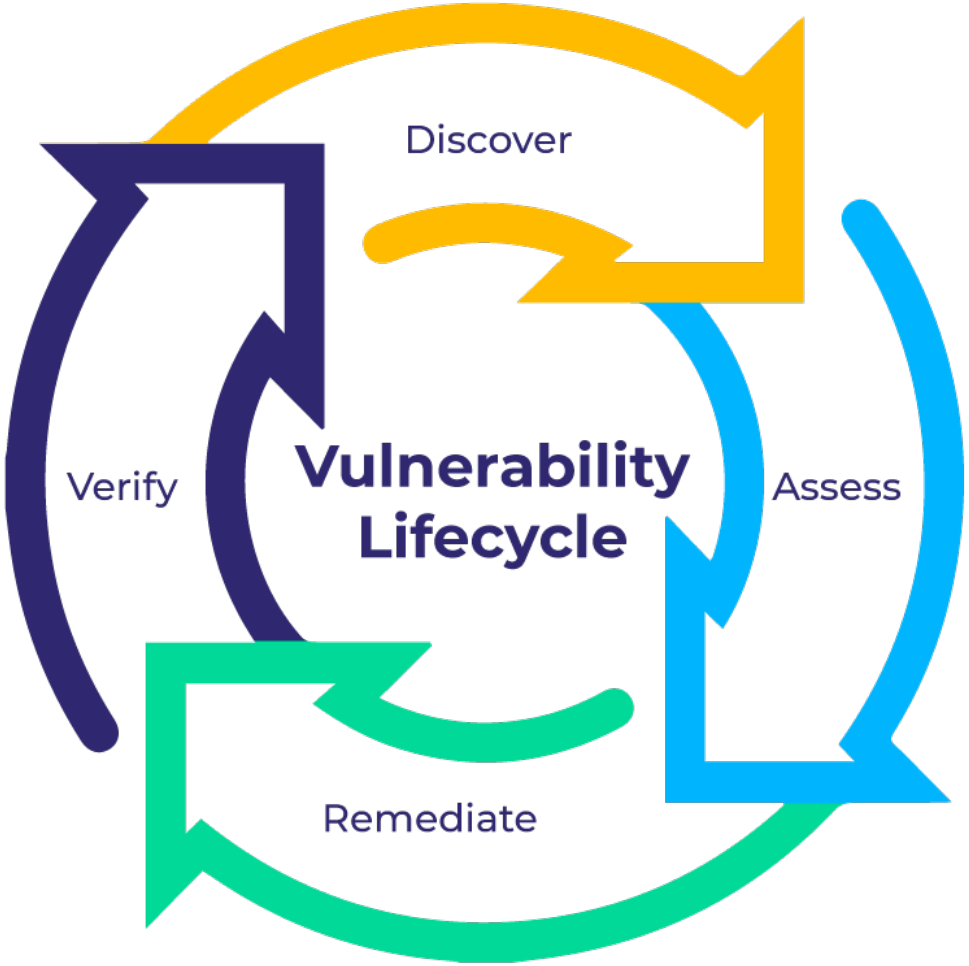
02 Мониторинг – разработка сценариев выявления

03 Средства защиты – разработка кастомных сигнатур

04 Киберучения / Red Teaming

05 Threat Intelligence – анализ и разработка

Уязвимости


Discover
Assess
Remediate
Verify
Vulnerability Lifecycle

Discovery

Источники:

01 Сканеры уязвимостей

02 Pentest

03 Threat Intelligence

04 Инциденты

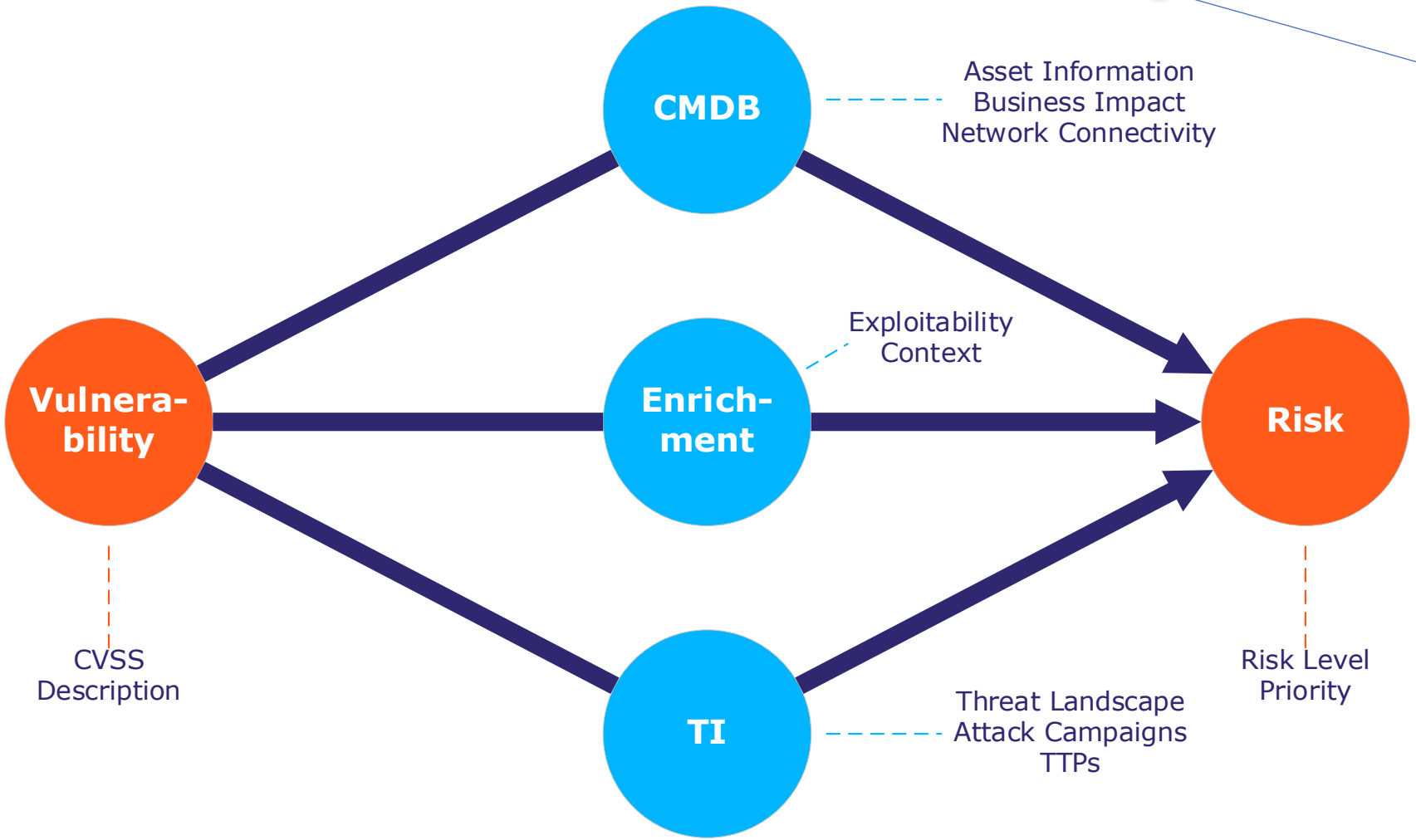
05 Бюллетени безопасности, новостные ресурсы, агрегаторы и т.д.

Discovery

Источники:

01	Сканеры уязвимостей
02	Pentest
03	Threat Intelligence
04	Инциденты
05	Бюллетени безопасности, новостные ресурсы, агрегаторы и т.д.

Assessment


CMDB
Asset Information
Business Impact
Network Connectivity
Vulnera-
bility
Enrich-
ment
Exploitability
Context
Risk
CVSS
Description
TI
Threat Landscape
Attack Campaigns
TTPs
Risk Level
Priority

Assessment

01 CMDB

02 Внешние источники

03 Threat Intelligence

Remediation

01 Установка обновления безопасности

02 Отключение уязвимого сервиса

03 Применение средства защиты

04 Изменение конфигурации / доступа

05 Мониторинг

Remediation

01 Установка обновления безопасности

02 Отключение уязвимого сервиса

03 Применение средств защиты

04 Изменение конфигурации / доступа

05 Мониторинг

Verify

01 Повторное сканирование

02 Повторный Pentest

03 Информация об установленных обновлениях

Реализация в SOAR

85 МИНУТ → 10 МИНУТЫ С SOAR

85 МИНУТ

ДО АВТОМАТИЗАЦИИ

35 мин | 25 мин | 15 мин | 10 мин

ПОЛУЧЕНИЕ ИНФОРМАЦИИ ОБ УЯЗВИМОСТИ

АНАЛИЗ КОНТЕКСТА УЯСВИМОСТИ

ОПРЕДЕЛЕНИЕ СТРАТЕГИИ УСТРАНЕНИЯ

УСТАНОВКА SLA, СОЗДАНИЕ ЗАЯВОК

КОНТРОЛЬ УСТРАНЕНИЯ И ПОДГОТОВКА ОТЧЕТА

ПОСЛЕ АВТОМАТИЗАЦИИ

10 МИНУТ

участие человека

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

СПАСИБО ЗА ВНИМАНИЕ