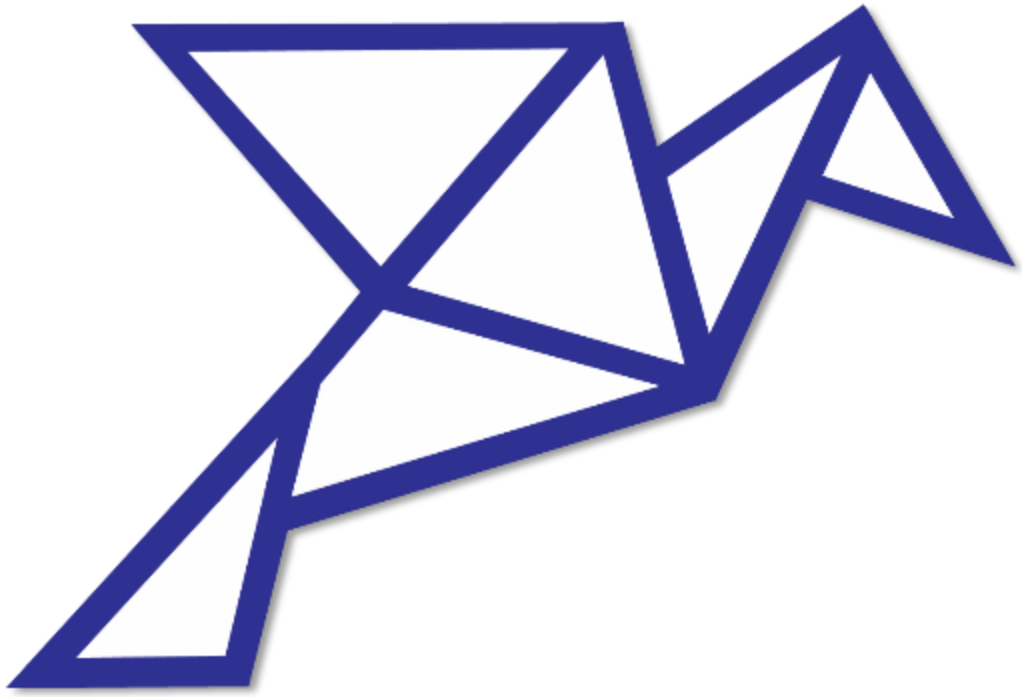
Cymulate BAS

Способ автоматизации тестирования средств ИБ



Кирилл Мурзин
Руководитель отдела ИБ

PACIFICA

Насколько эффективны ВАШИ средства защиты, люди и процессы?

Проблематика

- Полный функционал средств ИБ не используется
- Уязвимости из-за ошибок конфигураций
- Завышенные ожидания от вендора
- Не все векторы охвачены
- Современные атаки, техники атак и защиты не отслеживаются

Автоматизация vs Пентесты

Gartner выделил новый тип решений **BAS – Breach and Attack Simulation**
Июль 2017 г.

“Инструмент гарантирует повторяемость, лучшую отчетность и работает быстрее. Не говоря о том, что требует меньше навыков. **BAS и Red Team убьют пентесты”**
Августо Баррос, Gartner, Февраль 2018 г.

Cymulate получил статус **Cool Vendor в сегменте BAS**
Май 2018 г.

CYMULATE

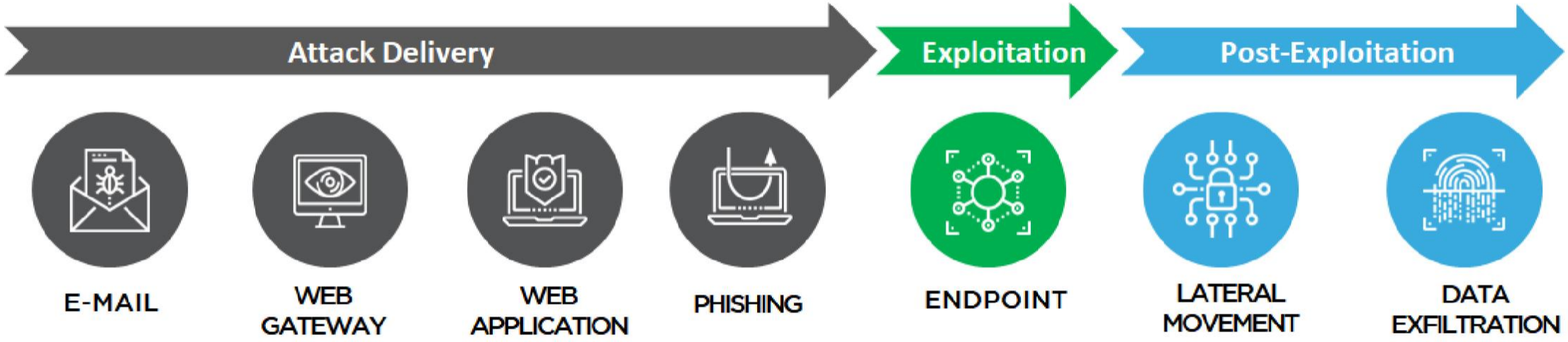
BREACH & ATTACK SIMULATION

- Cymulate была основана в 2016 году элитной командой бывших офицеров разведки IDF и ведущих кибер-исследователей, имеющих большой опыт в наступательных кибер-решениях.

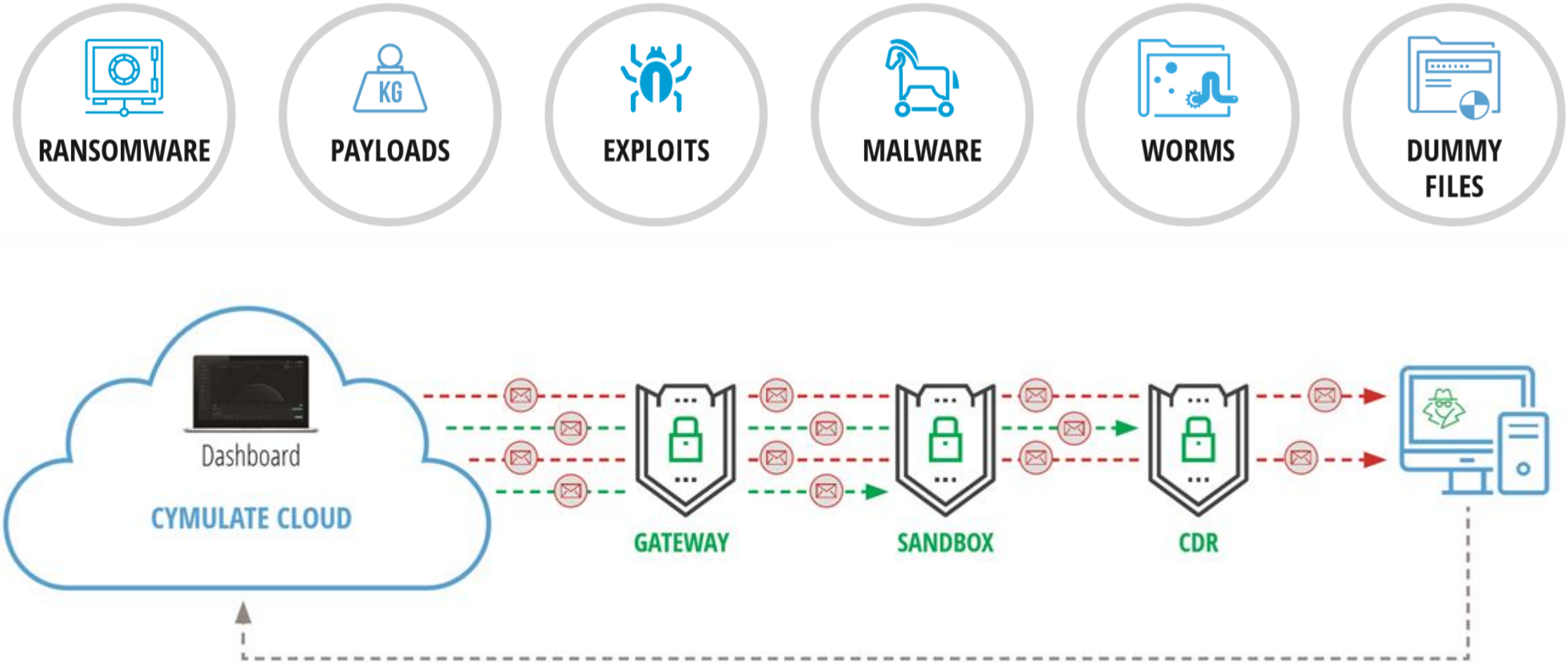
- Cymulate позволяет компаниям быть на шаг впереди киберпреступников с уникальной платформой имитации взлома и атак, которая помогает организациям улучшить их комплексные решения по безопасности.

- Подражая множеству стратегий, применяемых хакерами, система позволяет компаниям оценить свою истинную готовность эффективно противостоять угрозам кибербезопасности.

Стадии и вектора атак



Email & Web


RANSOMWARE
KG
PAYLOADS
EXPLOITS
MALWARE
WORMS
DUMMY FILES
Dashboard
CYMULATE CLOUD
GATEWAY
SANDBOX
CDR

Отчет по Email/Web

Разрешенные типы файлов

.pptx	.docx	.ics	.vcs	.pdf	.xlsx	.doc	.xls	.csv	.ppt	.dot	.rtf	.mdb	.acc..
.lnk	.eml	.html	.xsl	.xht..	.msg	.zip	.oft	.htm	.wav	.svg	.bat	.cmd	.com
.exe	.hta	.js	.jse	.pif	.scr	.vbe	.vbs	.wsf	.potm	.ppsm	.pptm	.slk	.xla
.xlam	.xlk	.xll	.xlm	.xlsb	.xlsm	.xlt	.xltm	.xlw	.xml	.docm	.dotm	.pot	.ppa
.ppam	.pps	.pwz	.sldm	.sldx	.wbk	.chm	.jar	.msi	.ods	.7z	.rar	.odt	.arj
.lha	.lzh	.tar	.gz	.cab	.UUE	.mp3	.pub						

Запрещенные типы файлов

.mcl

Отчет по Email/Web

Risk Level	Sent	Penetrated	%
High	507	145	29%
Medium	418	197	47%
Low	1968	1183	60%

Attack Type	Sent	Penetrated	%
Exploit	29	25	86%
Ransomware	403	120	30%
Malware	1185	585	49%
Worm	409	162	40%
Payload	413	212	51%
Dummy	444	411	93%
Links	10	10	100%

Отчет по Email/Web

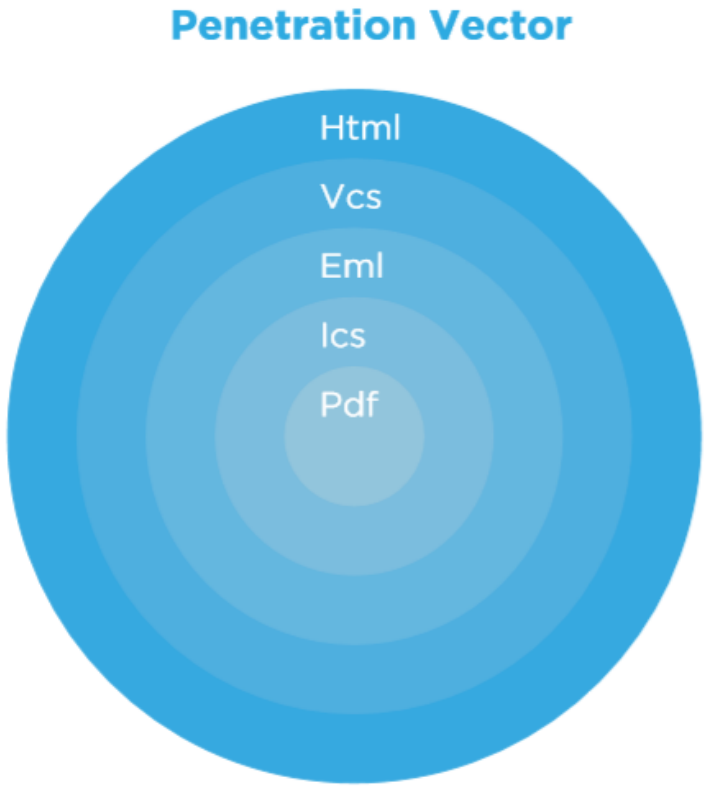
Adobe Util Printf PDF

AdobeutilprintfPdfIcsEmlVcsHtmlscript.html

Exploit

Similarity 100%

Low Risk



Описание:

Файл .**pdf** использует переполнение буфера в **Adobe Reader** и **Adobe Acrobat Professional <8.1.3.** Создав специально созданный **PDF-**файл, содержащий некорректную запись **util.printf (),** злоумышленник может выполнить произвольный код **Shellcode: MessageBox,** чтобы продемонстрировать концепцию выполнения кода.

СТАТИСТИКА CYMULATE ПО ОЦЕНКЕ EMAIL-ВЕКТОРА

49/100

средний процент успешности взлома (письма с крипто-локерами и вредоносами)

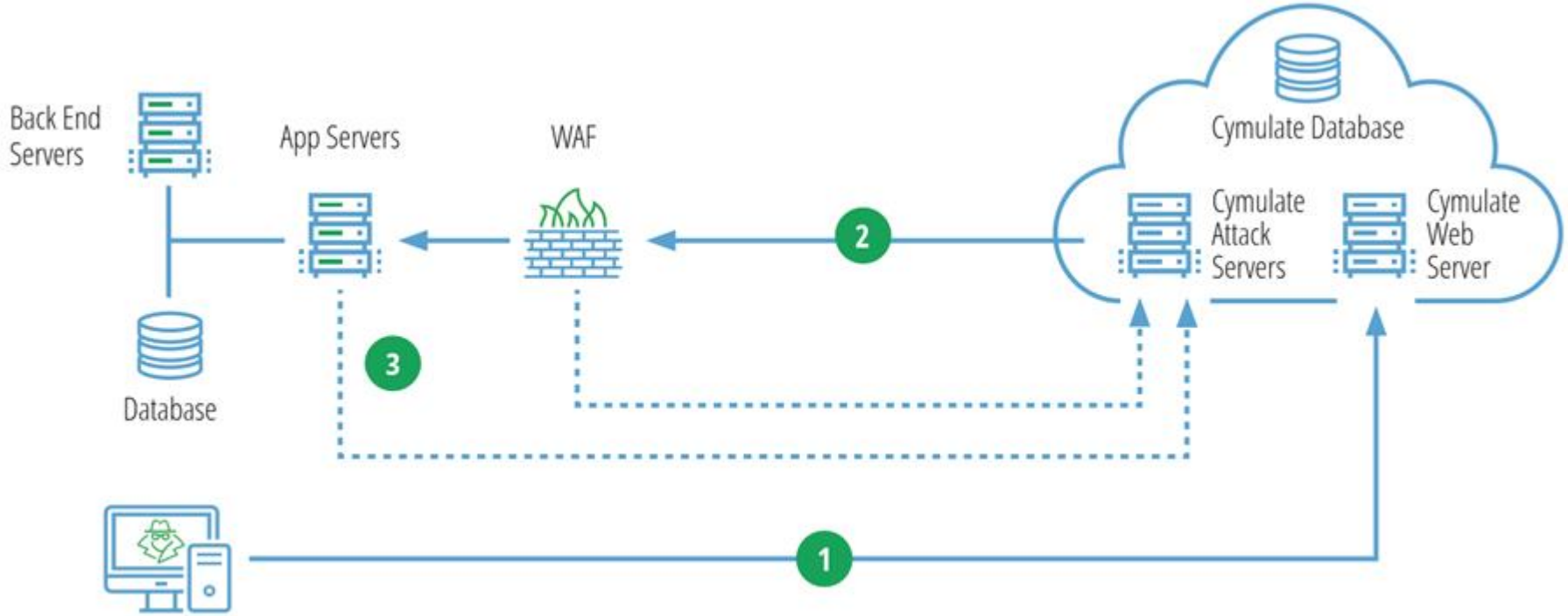
80%

организаций повышают уровень защищенности на треть за 2 часа

WAF


SQL-INJECTION
XSS
FILE INCLUSION
COMMAND INJECTION
VULNERABILITIES

WAF


Back End Servers
App Servers
WAF
Cymulate Database
Cymulate Attack Servers
Cymulate Web Server
Database
1
2
3

Отчет по WAF

Payload

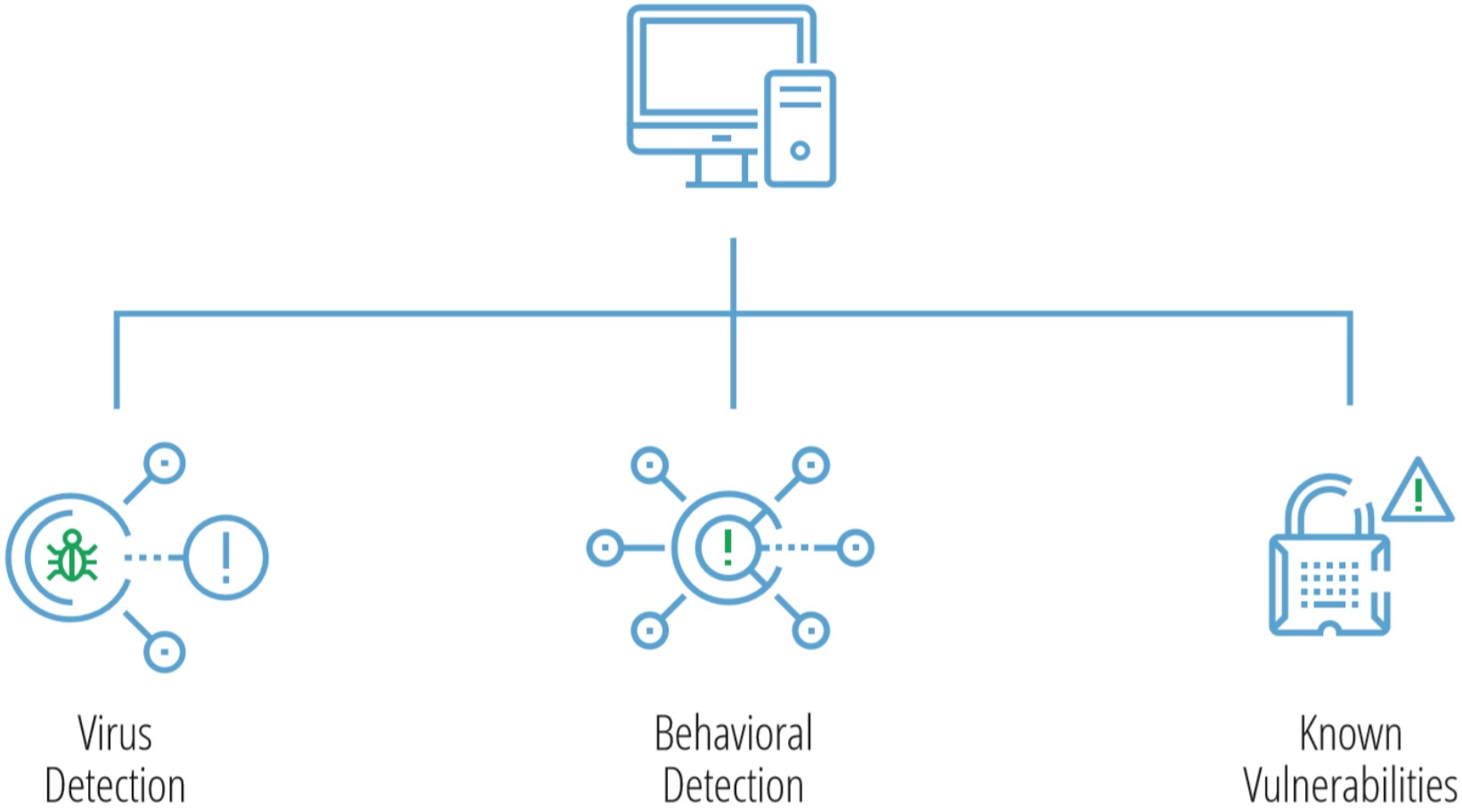
<iframe width="420" height="315" src="../../../../../../etc/passwd" frameborder="0" allowfullscreen></iframe>

URL

https://cymulate.com?ers41jxqjulk4tlh=<iframe width="420" height="315" src="../../../../../../etc/passwd" frameborder="0" allowfullscreen></iframe>

Описание
Атака обхода пути (также известная как обход каталога) предназначена для доступа к файлам и каталогам, которые хранятся вне корневой веб-папки. Управляя переменными, которые ссылаются на файлы с последовательностями «точка-точка-косая черта (../)» и их вариациями, или используя абсолютные пути к файлам.

Конечные точки

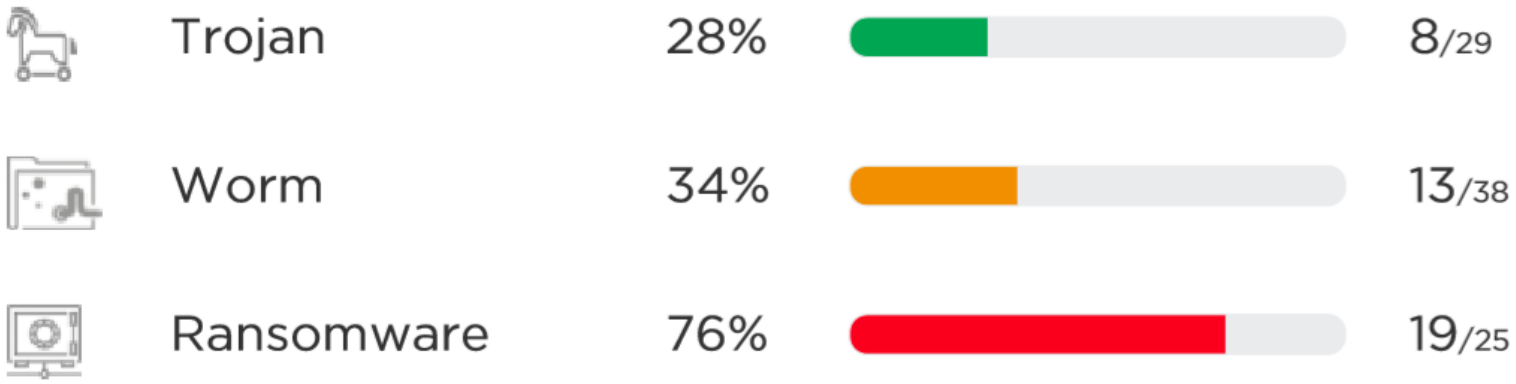


Отчет по конечным точкам

Attack Summary

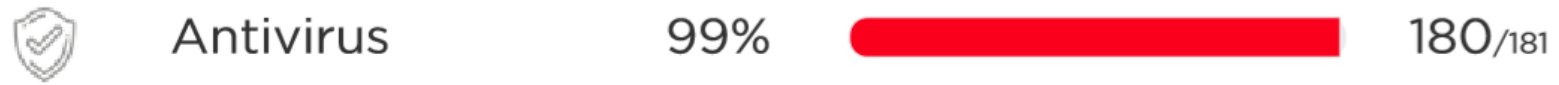
Behavior-based score breakdown

Percentage of completed attack scenarios



Signature-based score breakdown

percentage of unidentified malware samples



Отчет по конечным точкам

Ransomware - MSHTA - Ransomware Fixed Key

1/5  Executed	**Executing Payload Using MSHTA** ATT&CK Techniques Mshta	Using MSHTA.exe utility to execute the malicious HTA file.
2/5  Executed	**Found Folder**	2019-04-05 14:55:29 Locating target folder and scanning for files extensions to encrypt 26149
3/5  Executed	**Fixedkey**	2019-04-05 14:55:29 Encryption key: 26149
4/5  Executed	**Number Of Files Found** ATT&CK Techniques File and Directory Discovery	2019-04-05 14:55:29 51 files will be encrypted
5/5  Executed	**Encrypted**	2019-04-05 14:55:30 Encrypting all scanned files and compare the amount of scanned to successfully encrypted files

Внутреннее движение (Hopper)

Сбор информации с рабочих станций на основе MITRE ATT&CK framework с использованием различных инструментов и методов, таких как:

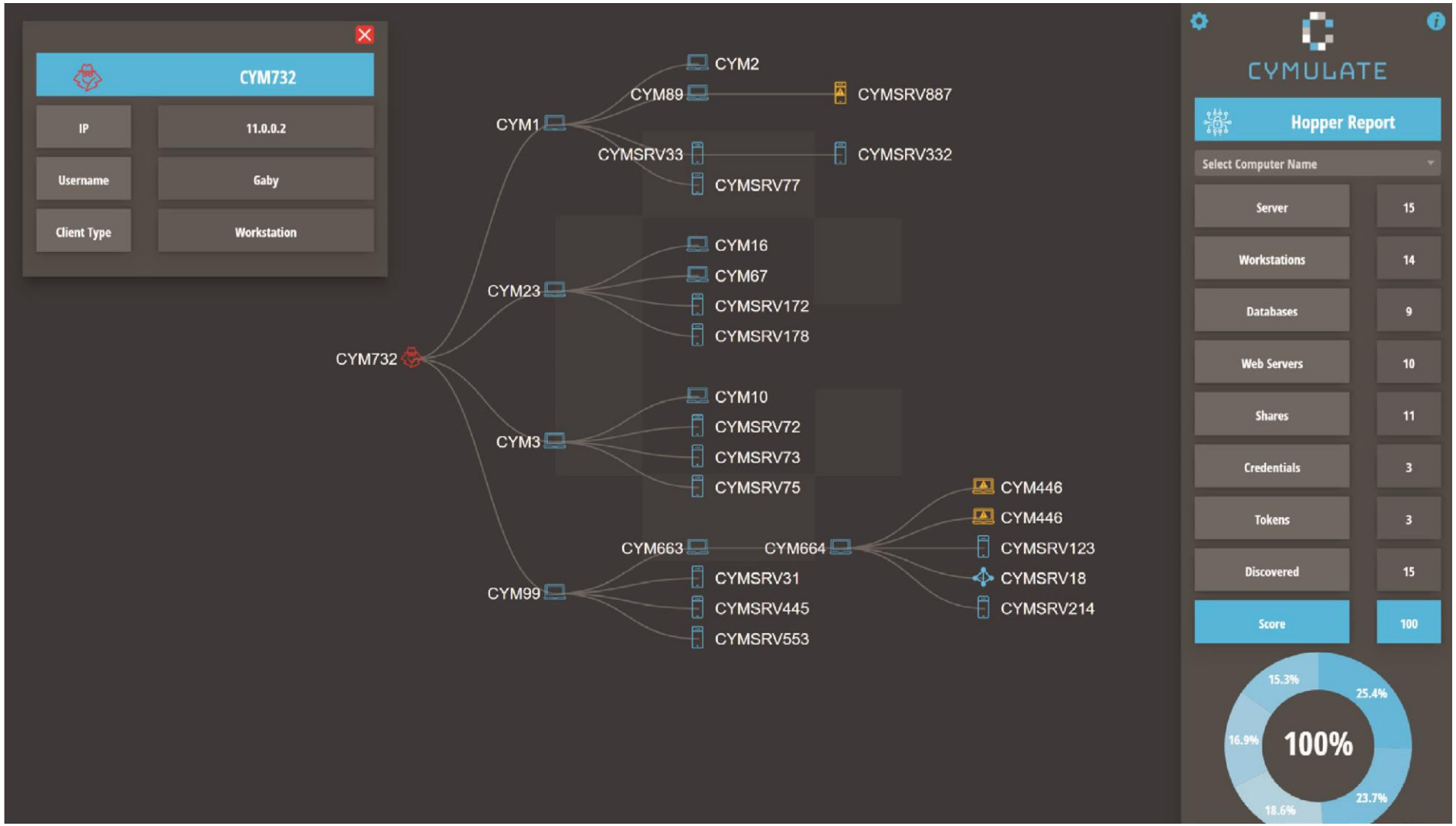
- MimiKatz – passwords/hashes/tokens from lsass, credentials manager
- Responder – NNLBT Poisoning
- Wide brute force

Сетевое сканирование

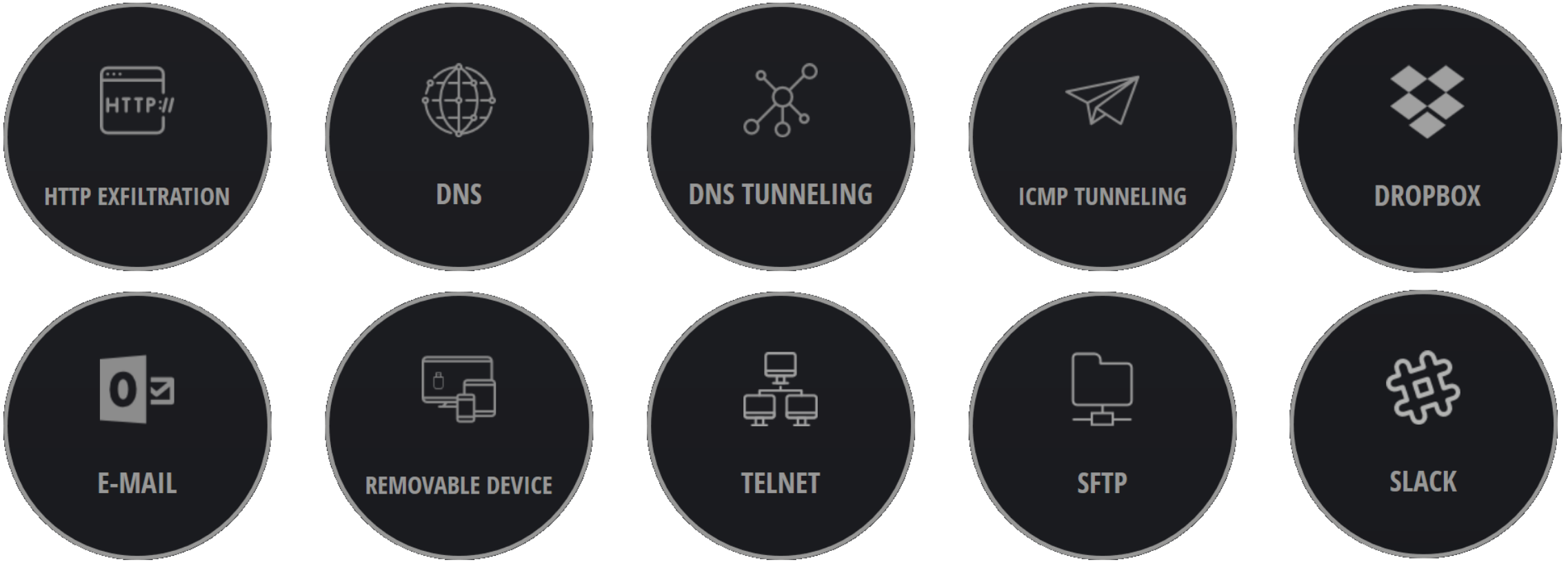
Распространение по сети через порты на основе полученной информации:

- SMB – port 445
- WMI – port 139
- DCOM – port 139
- RDP – port 3389

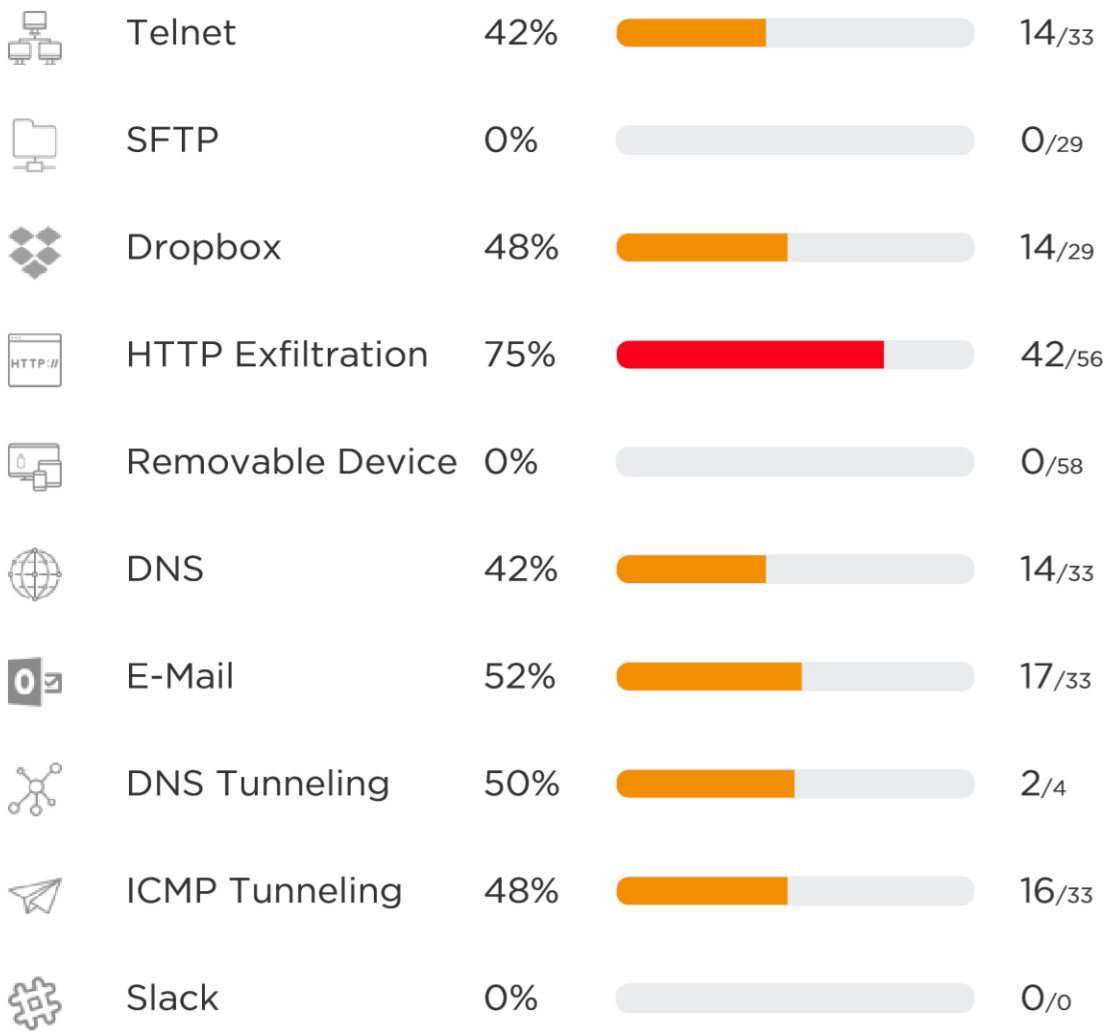
Отчет по Хопперу



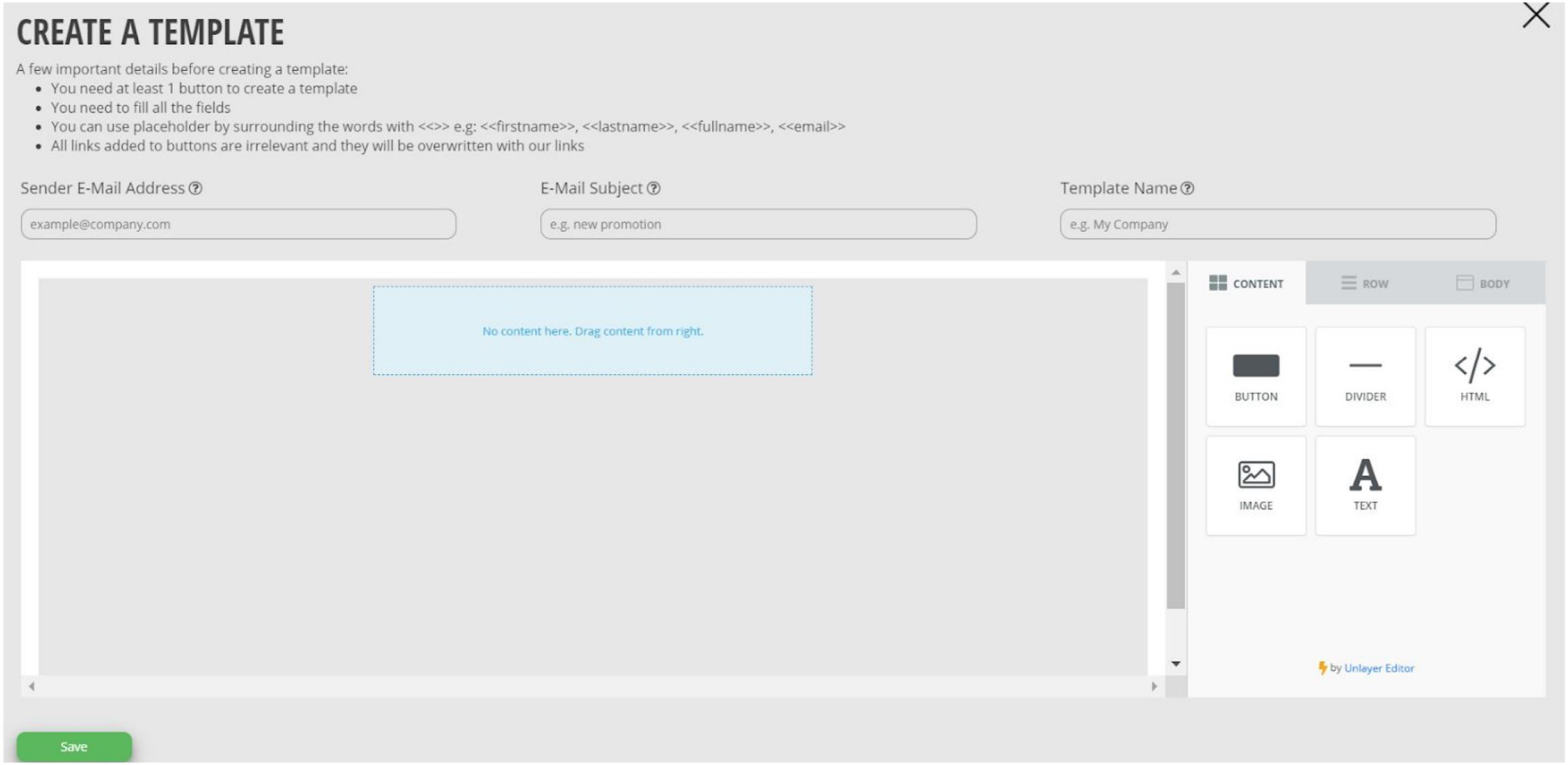
Эксфильтрация данных



Отчет по эксфильтрации данных



Фишинг


CREATE A TEMPLATE
A few important details before creating a template:
You need at least 1 button to create a template
You need to fill all the fields
You can use placeholder by surrounding the words with <<>> e.g: <<firstname>>, <<lastname>>, <<fullname>>, <<email>>
All links added to buttons are irrelevant and they will be overwritten with our links
Sender E-Mail Address
example@company.com
E-Mail Subject
e.g. new promotion
Template Name
e.g. My Company
No content here. Drag content from right.
CONTENT
ROW
BODY
BUTTON
DIVIDER
HTML
IMAGE
TEXT
by Unlayer Editor
Save

Отчет по фишингу

14

Участников

1/10

Ввели учетные данные

11/14

Открыли сообщение

7

Предыдущих участников

10/11

Перешли по ссылке

49/100

Успех кампании

Ключевые преимущества

- Комплексная оценка
- Кибер-устойчивость
- Моментальные результаты 24/7/365
- Оценка и оптимизация затрат на ИБ
- Сервисная модель
- Не влияет на бизнес-процессы

Рекомендации

- Провести инвентаризацию и аудит политик средств ИБ
- Выявить пробелы и расставить приоритеты
- Устранить проблемы и перепроверить
- Проводить тестирования на регулярной основе
- Инвестировать в квалификацию персонала

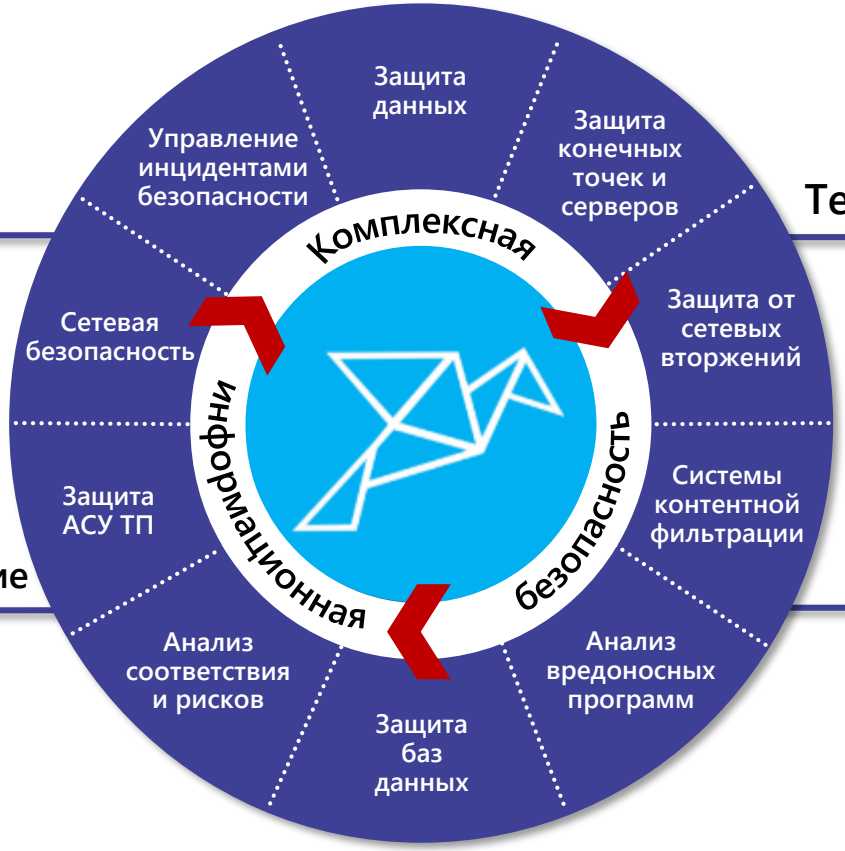
Направления деятельности

Аудит и консалтинг

- Подготовка к аудиту в соответствии с международными стандартами (ISO 27001, PA/PCI DSS)
- Консультации по вопросам обеспечения информационной безопасности

Проектирование и внедрение

- Проектирование и внедрение систем информационной безопасности
- Построение центра управления инцидентами, защита центров обработки данных (ЦОД)
- Проектирование и построение ИТ-инфраструктуры и инженерных систем ЦОД, офисов, зданий и сооружений. Внедрение систем безопасности



Техподдержка и аутсорсинг

- Поддержка и сопровождение систем информационной безопасности (СИБ)
- Оптимизация ИБ-инфраструктуры, ИБ-аутсорсинг, облачные ИБ-сервисы

Обучение

- Проведение тренингов и обучающих семинаров менеджеров и технических специалистов ИБ
- Обучение специалистов ИБ по собственным программам

ТОО «ПАЦИФИКА» предоставляет комплекс решений и услуг, позволяющих нашим клиентам выстраивать систему обеспечения информационной безопасности и ИТ-инфраструктуру «с нуля» или оптимизировать существующую

Наши контакты

Алматы	ул. Ауэзова 60, БЦ «Almaty Residence», 6-й этаж, офис 17А тел. +7 (727) 355 00 11
Нур-Султан	ул. Д.Кунаева 29/1, гостиница «Дипломат», офис 1906 тел. +7 (7172) 28 00 82
Атырау	ул. Сары Арка 40, офис 230 тел. +7 (777) 771 79 69
Москва	ул. Верейская, дом 5, 2-й этаж, помещение 1, комната №10 тел. +7 (495) 745 77 88

info@pacifica.kz

facebook.com/pacifica.kz

https://www.pacifica.kz

PACIFICA

www.pacifica.kz