Threat Intelligence Feeds

Описание продукта

Дата редакции документа: 31.05.2024

Содержание

1. Общие сведения

PT Threat Intelligence Feeds (PT Feeds) позволяет командам SOC быть в курсе актуальных угроз ИБ. Продукт содержит широкий спектр индикаторов компрометации, включая:

— домены,

— IP-адреса,

— ссылки,

— хеш-суммы файлов.

Экспертизу PT Feeds формируют эксперты PT ESC, используя материалы расследований инцидентов, исследований хакерских группировок, а также обезличенные данные продуктов Positive Technologies.

2. Особенности и преимущества

Уникальные данные о реальных угрозах

Обезличенная телеметрия с сотен инсталляций продуктов Positive Technologies позволяет формировать знания о том, что происходит в мире ИБ прямо сейчас.

Репутация и оценка потенциального ущерба

Для каждого индикатора компрометации рассчитываются показатели «Репутация» и «Потенциальный ущерб». Это помогает приоритизировать угрозы, оценить возможный ущерб от их реализации и сфокусироваться на предотвращении самых опасных из них.

Расширенные контекстные данные

Обогащение индикаторов компрометации дополнительными данными помогает аналитикам SOC принимать решения по реагированию на угрозы.

Более 40 фидов

Индикаторы компрометации в составе PT Feeds объединены в коллекции по целям их применения: для таргетированных атак, относящиеся к определенным семействам ВПО, конкретным вредоносным кампаниям и т. д.

Интеграция с продуктами разных вендоров

PT Feeds поддерживает разные форматы и широкий перечень средств защиты информации, который постоянно дополняется.

3. Доступный перечень фидов

В таблице ниже представлен доступный заказчикам перечень потоков данных с индикаторами компрометации. Перечень приведен для демонстрации возможных срезов данных репутационного сервиса Positive Technologies. По запросу заказчика могут быть сформированы индивидуальные потоки данных.

Таблица 1. Доступный перечень фидов

№	Наименование	Описание	Назначение
1	Malicious domains, URLs, IPs, hashes	Вредоносные индикаторы без дополнительной разметки	Фид предназначен для детектирования угроз без необходимости в дополнительной приоритизации и контексте. Актуально для любых детектирующих классов СЗИ
2	White list domains, URLs, IPs, hashes	Белый список индикаторов	Фид предназначен для формирования белых списков индикаторов для уменьшения количества ложноположительных срабатываний. Актуально для любых детектирующих классов СЗИ. **IRP, SOAR** — фид может использоваться для категоризации индикаторов, обнаруженных в процессе реагирования на инцидент или его расследования. Категоризация может служить как для приоритизации инцидента, так и для ускорения его расследования (не потребуется тратить время на уточнение информации об индикаторе)

№	Наименование	Описание	Назначение
3	High severity domains, URLs, IPs, hashes	Вредоносные индикаторы высокой степени опасности с точки зрения влияния на инфраструктуру предприятия	1. **IDS, NTA, NGFW** — для детектирования наиболее опасных индикаторов на периметре сетевой инфраструктуры компании. 2. **SIEM** — для приоритизации срабатываний (чем критичнее индикатор, тем более высокий приоритет инцидента). 3. **IRP, SOAR** — для обогащения контекста карточки инцидента и выстраивания цепочек связанных индикаторов (с помощью поля relations). 4. **EDR** — для приоритетного сканирования системы и удаления вредоносных образцов
4	Medium severity domains, URLs, IPs, hashes	Вредоносные индикаторы средней степени опасности с точки зрения влияния на инфраструктуру предприятия	
5	Current activity domains, URLs, IPs, hashes	Вредоносные индикаторы, активные за последнюю неделю	1. **IDS, NTA, NGFW** — для детектирования наиболее актуальных (активных недавно) индикаторов на периметре сетевой инфраструктуры компании. 2. **SIEM** — для приоритизации срабатываний (чем актуальнее индикатор, тем выше вероятность, что он «живой» и тем более высокий приоритет инцидента). 3. **IRP, SOAR** — для обогащения контекста карточки инцидента. 4. **EDR** — для приоритетного сканирования системы и удаления вредоносных образцов
6	Recent activity domains, URLs, IPs, hashes	Вредоносные индикаторы, активные за последний месяц	
7	Retrospective domains, URLs, IPs, hashes	Вредоносные индикаторы, активные за последний год	Фид предназначен для реализации сценариев threat hunting.

№	Наименование	Описание	Назначение
			Фид может быть использован в различных СЗИ, а также других инфраструктурных сервисах для поиска событий с участием представленных в фиде индикаторов. Например, фид retrospective IPs может быть использован для поиска событий в NetFlow и журналах FW или NGFW, фид retrospective domains — в NTA и журналах DNS, а фид retrospective hashes — для анализа почтовых вложений в SEG-решениях, а также для сканирования конечных узлов с помощью EDR
8	Current activity severity domains, URLs, IPs, hashes	Вредоносные индикаторы с разметкой по степени опасности, активные за последнюю неделю	Объединение фидов activity и severity, позволяющее еще более тонко настраивать приоритетность детектов.
9	Recent activity severity domains, URLs, IPs, hashes	Вредоносные индикаторы с разметкой по степени опасности, активные за последний месяц	Назначение этих фидов аналогично фидам типа activity и severity: 1. **IDS, NTA, NGFW** — для детектирования наиболее актуальных и опасных индикаторов на периметре сетевой инфраструктуры компании. 2. **SIEM** — для приоритизации срабатываний (чем актуальнее и опаснее индикатор, тем выше приоритет инцидента). 3. **IRP, SOAR** — для обогащения контекста в карточке инцидента и выстраивания цепочек связанных индикаторов (с помощью поля relations). 4. **EDR** — для приоритетного сканирования системы и удаления вредоносных образцов

№	Наименование	Описание	Назначение
10	Retrospective severity domains, URLs, IPs, hashes	Вредоносные индикаторы с разметкой по степени опасности, активные за последний год	Фид предназначен для реализации сценариев threat hunting. Фид позволяет проводить более быстрый и точечный ретроспективный анализ — ориентироваться на индикаторы с определенным уровнем актуальности или опасности. Фид может быть использован в различных СЗИ, а также других инфраструктурных сервисах для поиска событий с представленными в фиде индикаторами. Например, фид Retrospective IPs может быть использован для поиска событий в NetFlow и журналах FW или NGFW, Retrospective domains feed — в NTA и журналах DNS, а Retrospective hashes feed — для анализа почтовых вложений в SEG-решениях, а также для сканирования конечных узлов с помощью EDR
11	TOR IPs	IP-адреса, размеченные как TOR Node	1. **NGFW** — для применения политики безопасности на межсетевом экране, в зависимости от которой взаимодействие с определенными типами сетевых ресурсов может быть разрешено, заблокировано или задетектировано на СЗИ. 2. **IRP, SOAR** — для категоризации индикаторов, обнаруженных в процессе реагирования на инцидент или его расследования. Категоризация может служить как для приоритизации инцидента, так и для ускорения его обработки (не потребуется тратить время на уточнение информации об индикаторе)
12	DynDNS domains	Домены, относящиеся к инфраструктуре DynDNS	
13	Cloud IPs, IP ranges	IP-адреса, относящиеся к облачной инфраструктуре	
14	VPN IPs, IP ranges	IP-адреса, относящиеся к VPN	
15	STUN IPs	IP-адреса STUN-серверов	
16	Sinkhole IPs, IP ranges	IP-адреса, размеченные как узлы sinkhole	
17	Mail domains	Домены, относящиеся к почтовой инфраструктуре	
18	CDN domains, IPs, IP ranges, URLs	Вредоносные домены, URL и IP-адреса, относящиеся к CDN инфраструктуре	

№	Наименование	Описание	Назначение
19	Torrents domains, IPs, URLs	Вредоносные домены, URL и IP-адреса, относящиеся к торрент-трекерам	
20	Proxy domains, IPs, URLs	Вредоносные домены, URL и IP-адреса, относящиеся к инфраструктуре proxy	
21	Scanners IPs	Перечень IP-адресов, относящихся к сервисам, которые собирают информацию об открытых сетевых ресурсах	
22	Service domains, IPs, URLs	Домены, URL, IP-адреса, относящиеся к различным сервисам	
23	Cryptomining domains, URLs, IPs	Вредоносные сетевые индикаторы, связанные с криптомайнингом	
24	Exploiters IPs	IP-адреса, связанные с эксплуатацией уязвимостей	1. **SIEM** — для определения стадии развития атаки на инфраструктуру компании. Например, если получен детект вредоносного сетевого ресурса с ролью phishing, то атака на стадии delivery (initial access), а если с ролью upload, то на стадии actions on objectives (exfiltration). 2. **SIEM** — для приоритизации инцидентов в зависимости от ландшафта угроз компании. Например, если организация считает наиболее опасным вектором атаки фишинг, инциденты, связанные с детектами индикаторов с ролью phishing, будут иметь высокий приоритет. 3. **NGFW, DLP** — для детектирования утечек информации. Наличие сетевых детектов, связанных с
25	CnC malicious domains, URLs, IPs	Вредоносные домены, URL и IP-адреса, связанные с управляющими серверами злоумышленников	
26	Phishing malicious domains, URLs, IPs	Вредоносные домены, URL и IP-адреса, связанные с фишинговыми ресурсами злоумышленников	
27	Download malicious domains, URLs, IPs	Вредоносные домены, URL и IP-адреса, используемые злоумышленниками для скачивания полезной нагрузки	
28	Upload malicious domains, URLs, IPs	Вредоносные домены, URL и IP-адреса, используемые злоумышленниками для эксфильтрации данных	

№	Наименование	Описание	Назначение
			индикаторами с ролью upload, может свидетельствовать об утечке данных. 4. **IRP, SOAR** — для обогащения контекста карточки инцидента
29	Malicious class domains, URLs, IPs, hashes	Вредоносные индикаторы, размеченные по классам ВПО	1. **SIEM** — для приоритизации инцидентов в зависимости от ландшафта угроз компании. Например, если организация считает наиболее опасным классом ВПО вирусы-вымогатели, то инциденты, связанные с обнаружением индикаторов с этим классом, будут иметь высокий приоритет. 2. **IRP, SOAR** — для обогащения контекста в карточке инцидента и выстраивания цепочек связанных индикаторов (с помощью поля relation). 3. **EDR** — индикаторы наиболее опасных для компании классов могут использоваться для приоритетного сканирования системы и удаления вредоносных образцов. 4. **IDS, NTA, NGFW** — для детектирования индикаторов наиболее опасных для компании классов ВПО на периметре сетевой инфраструктуры
30	Malicious class current activity	Вредоносные индикаторы, размеченные по классам ВПО, активные за послед-нюю неделю	Объединение фидов классов activity и malicious, позволяющее еще более тонко настраивать приоритетность детектов
31	Malicious class recent activity	Вредоносные индикаторы, размеченные по классам ВПО, активные за последний месяц	

№	Наименование	Описание	Назначение
			Назначение фидов аналогично назначению фидов классов activity и malicious: 1. **IDS, NTA, NGFW** — для детектирования наиболее актуальных индикаторов на периметре сетевой инфраструктуры компании с учетом уровня опасности классов ВПО в рамках ландшафта угроз. 2. **SIEM** — для приоритизации срабатываний (чем актуальнее индикатор с точки зрения времени активности и класса ВПО, тем выше приоритет инцидента). 3. **IRP, SOAR** — для обогащения контекста в карточке инцидента и выстраивания цепочек связанных индикаторов (с помощью поля relations). 4. **EDR** — для приоритетного сканирования системы и удаления вредоносных образцов
32	Malicious class retrospective	Вредоносные индикаторы, размеченные по классам ВПО, активные за последний год	Фид предназначен для реализации сценариев threat hunting. Фид позволяет проводить более быстрый и точечный ретроспективный анализ — ориентироваться на индикаторы с определенным уровнем актуальности или опасности. Фид может быть использован в различных СЗИ, а также других инфраструктурных сервисах для поиска событий с представленными в фиде индикаторами. Например, фид retrospective IPs может быть использован для поиска событий в NetFlow и журналах FW или NGFW, фид retrospective

№	Наименование	Описание	Назначение
			domains — в NTA и журналах DNS, а фид retrospective hashes — для анализа почтовых вложений в SEG-решениях, а также для сканирования конечных узлов с помощью EDR
33	Malicious family domains, URLs, IPs, hashes	Вредоносные индикаторы, размеченные по семействам ВПО	1. **SIEM** — для приоритизации инцидентов в зависимости от ландшафта угроз компании. Например, если организация считает наиболее опасным семейством ВПО Emotet, то инциденты, связанные с детектами индикаторов с этим классом, будут иметь высокий приоритет. 2. **IRP, SOAR** — для обогащения контекста в карточке инцидента и выстраивания цепочек связанных индикаторов (с помощью поля relations). 3. **EDR** — для приоритетного сканирования системы и удаления вредоносных образцов. 4. **IDS, NTA, NGFW** — для детектирования индикаторов наиболее опасных для компании семейств ВПО на периметре сетевой инфраструктуры
34	Malicious family current activity	Вредоносные индикаторы, размеченные по семействам ВПО, активные за последнюю неделю	Объединение фидов activity и malicious family, позволяющее еще более тонко настраивать приоритетность детектов. Назначение этих фидов аналогично фидам activity и malicious family: 1. **IDS, NTA, NGFW** — для детектирования наиболее актуальных индикаторов на периметре сетевой инфраструктуры компании с
35	Malicious family recent activity	Вредоносные индикаторы, размеченные по семействам ВПО, активные за последний месяц	

№	Наименование	Описание	Назначение
			учетом уровня опасности семейств ВПО в рамках ландшафта угроз. 2. **SIEM** — для приоритизации срабатываний (чем актуальнее индикатор с точки зрения времени активности и семейства ВПО, тем выше приоритет инцидента). 3. **IRP, SOAR** — для обогащения контекста в карточке инцидента и выстраивания цепочек связанных индикаторов (с помощью поля relations). 4. **EDR** — для приоритетного сканирования системы и удаления вредоносных образцов
36	Malicious family retrospective	Вредоносные индикаторы, размеченные по семействам ВПО, активные за последний год	Фид предназначен для реализации сценариев threat hunting. Фид позволяет проводить более быстрый и точечный ретроспективный анализ — ориентироваться на индикаторы с определенным уровнем актуальности или опасности. Фид может быть использован в различных СЗИ, а также других инфраструктурных сервисах для поиска событий с представленными в фиде индикаторами. Например, фид malicious group retrospective IPs может быть использован для поиска событий в NetFlow и журналах FW или NGFW, фид malicious group retrospective domains — в NTA и журналах DNS, а фид malicious group retrospective hashes — для анализа почтовых вложений в SEG-решениях, а также для сканирования конечных узлов с помощью EDR

№	Наименование	Описание	Назначение
37	Malicious campaign domains, URLs, IPs, hashes	Вредоносные индикаторы, агрегированные по вредоносным кампаниям	1. **SIEM** — для приоритизации инцидентов в зависимости от вредоносной кампании, к которой относится индикатор. Например, приоритетными могут считаться все инциденты, маркированные индикаторами, связанными с какой-либо вредоносной кампанией. Либо в качестве приоритетных могут рассматриваться инциденты, индикаторы которых связаны с вредоносными кампаниями, направленными на страну или отрасль организации. 2. **IRP, SOAR** — для обогащения контекста в карточке инцидента и выстраивания цепочек связанных индикаторов (с помощью поля relations). 3. **EDR** — для приоритетного сканирования системы и удаления вредоносных образцов. 4. **IDS, NTA, NGFW** — для детектирования на периметре сетевой инфраструктуры индикаторов, наиболее опасных с точки зрения вредоносных кампаний
38	Malicious campaign current activity	Вредоносные индикаторы, агрегированные по вредоносным кампаниям, активные за последнюю неделю	Объединение фидов activity и malicious campaign, позволяющее еще более тонко настраивать приоритетность детектов. Назначение этих фидов аналогично фидам activity и malicious campaign: 1. **IDS, NTA, NGFW** — для детектирования наиболее актуальных индикаторов на периметре сетевой инфраструктуры компании с
39	Malicious campaign recent activity	Вредоносные индикаторы, агрегированные по вредоносным кампаниям, активные за последний месяц	

№	Наименование	Описание	Назначение
			учетом уровня опасности вредоносных кампаний в рамках ландшафта угроз. 2. **SIEM** — для приоритизации срабатываний (чем актуальнее индикатор с точки зрения времени активности и вредоносной кампании, тем выше приоритет инцидента). 3. **IRP, SOAR** — для обогащения контекста карточки инцидента и выстраивания цепочек связанных индикаторов (с помощью поля relations). 4. **EDR** — наиболее актуальные (с точки зрения времени активности и вредоносной кампании) файловые индикаторы могут использоваться для приоритетного сканирования системы и удаления вредоносных образцов
40	Malicious campaign retrospective	Вредоносные индикаторы, агрегированные по вредоносным кампаниям, активные за последний год	Фид предназначен для реализации сценариев threat hunting. Фид позволяет проводить более быстрый и точечный ретроспективный анализ — ориентироваться на индикаторы с определенным уровнем актуальности или опасности. Фид может быть использован в различных СЗИ, а также других инфраструктурных сервисах для поиска событий с представленными в фиде индикаторами. Например, фид malicious campaign retrospective IPs может быть использован для поиска событий в NetFlow и журналах FW или NGFW, фид malicious campaign retrospective domains — в NTA и журналах DNS, а фид malicious campaign retrospective

№	Наименование	Описание	Назначение
			hashes — для анализа почтовых вложений в SEG-решениях, а также для сканирования конечных узлов с помощью EDR
41	Malicious group domains, URLs, IPs, hashes	Вредоносные индикаторы с разметкой по группировкам	1. **SIEM** — для приоритизации инцидентов в зависимости от ландшафта угроз компании. Например, если организация считает наиболее опасной для себя группировкой Lazarus, то инциденты, связанные с детектами индикаторов этой группировки, будут иметь высокий приоритет. 2. **IRP, SOAR** — для обогащения контекста в карточке инцидента и выстраивания цепочек связанных индикаторов (с помощью поля relations). 3. **EDR** — для приоритетного сканирования системы и удаления вредоносных образцов. 4. **IDS, NTA, NGFW** — для детектирования индикаторов наиболее опасных для компании группировок на периметре сетевой инфраструктуры
42	Malicious group current activity	Вредоносные индикаторы с разметкой по группировкам, активные за последнюю неделю	Объединение фидов activity и malicious group, позволяющее еще более тонко настраивать приоритетность детектов. Назначение этих фидов: 1. **IDS, NTA, NGFW** — для детектирования наиболее актуальных индикаторов на периметре сетевой инфраструктуры компании с
43	Malicious group recent activity	Вредоносные индикаторы с разметкой по группировкам, активные за последний месяц	

№	Наименование	Описание	Назначение
			учетом уровня опасности группировок в рамках ландшафта угроз. 2. **SIEM** — для приоритизации срабатываний (чем актуальнее индикатор с точки зрения времени активности и группировки, тем выше приоритет инцидента). 3. **IRP, SOAR** — для обогащения контекста в карточке инцидента и выстраивания цепочек связанных индикаторов (с помощью поля relations). 4. **EDR** — для приоритетного сканирования системы и удаления вредоносных образцов
44	Malicious group retrospective	Вредоносные индикаторы с разметкой по группировкам, активные за последний год	Фид предназначен для реализации сценариев threat hunting. Фид позволяет проводить более быстрый и точечный ретроспективный анализ — ориентироваться на индикаторы с определенным уровнем актуальности или опасности. Фид может быть использован в различных СЗИ, а также других инфраструктурных сервисах для поиска событий с представленными в фиде индикаторами. Например, фид malicious group retrospective IPs может быть использован для поиска событий в NetFlow и журналах FW или NGFW, фид malicious group retrospective domains — в NTA и журналах DNS, а фид malicious group retrospective hashes — для анализа почтовых вложений в SEG-решениях, а также для сканирования конечных узлов с помощью EDR

№	Наименование	Описание	Назначение
45	Cybercrime domains, URLs, IPs, hashes	Вредоносные индикаторы, связанные с массовыми угрозами	1. **SIEM** — для приоритизации срабатываний СЗИ. Инциденты, связанные с атаками APT группировок, могут получать более высокий приоритет. 2. **IRP, SOAR** — для обогащения контекста в карточке инцидента и выстраивания цепочек связанных индикаторов (с помощью поля relations)
46	APT domains, URLs, IPs, hashes	Вредоносные индикаторы, связанные с целевыми угрозами	
47	Geo anomaly IPs	IP-адреса, размеченные по GeoIP, без узлов, связанных с VPN, прокси, STUN, Tor, DynDNS	**NGFW** — для применения политики безопасности на межсетевом экране, в зависимости от которой доступ к внутренней сетевой инфраструктуре из определенных стран может быть разрешен, заблокирован или задетектирован на СЗИ
48	FinCERT domains, URLs, IPs, hashes	Вредоносные индикаторы, передаваемые по линии ФинЦЕРТ	Детектирования угроз на базе индикаторов, поставляемых из «ФинЦЕРТ». Актуально для любых детектирующих классов СЗИ

4. Перечень атрибутов объектов

Ниже представлены атрибуты объектов, которые могут быть описаны в коллекции. Список не является исчерпывающим и может корректироваться в зависимости от схемы, согласно которой формируется коллекция.

Общий список атрибутов индикаторов компрометации:

- Репутация индикатора на момент выгрузки.
- Итоговый вердикт.
- Временные метки.
- Принадлежность или связь:
  - с классом вредоносного ПО,
  - с семейством вредоносного ПО,
  - с группировками APT / киберпреступностью,
  - с вредоносной кампанией.
- Потенциальный ущерб — опасность угрозы, связанной с индикатором, для инфраструктуры организации.
- Роли узла в сети.
- Доступность домена или IP-адреса.
- Вердикты антивирусов и песочниц.
- Результаты обогащений с помощью WHOIS/DNS.

Детальные описания атрибутов каждой сущности приведены ниже.

В этом разделе

4.1. Итоговые вердикты по индикаторам

Класс `Verdict` — это перечисление, объекты которого принимают следующие значения:

- `unscored` — вердикт индикатора не определен;
- `suspicious` — подозрительный индикатор, который нельзя явно отнести к `clean` или `malicious`;
- `clean` — индикатор, признанный безопасным по итогам анализа контекста;

— `malicious` — вредоносный индикатор;
— `whitelisted` — индикатор, признанный безопасным на основе белых списков;
— `torrent_tracker` — индикатор, связанный с инфраструктурой торрент-трекеров;
— `sinkhole` — индикатор, относящийся к sinkhole-узлам;
— `parking` — индикатор, используемый для парковки незарегистрированных доменов;
— `public_dns_server` — индикатор, относящийся к общедоступным DNS-серверам;
— `scanner` — индикатор, связанный с активностью сканеров сетевых ресурсов;
— `cloud` — индикатор, относящийся к облачной инфраструктуре крупных компаний;
— `stun` — индикатор, относящийся к STUN-серверам;
— `tor_node` — индикатор, относящийся к узлам Tor;
— `crawler` — индикатор, относящийся к краулерам информации веб-сервисов;
— `cdn` — индикатор, относящийся к инфраструктуре CDN;
— `vpn_gate` — индикатор, относящийся к инфраструктуре VPN;
— `proxy` — индикатор, относящийся к прокси-инфраструктуре;
— `exploiter` — индикатор, связанный с эксплуатацией уязвимостей.

4.2. Роль сетевого индикатора в инфраструктуре злоумышленника

Класс `Role` — это перечисление, объекты которого принимают следующие значения:

— `unknown` — роль узла не определена;
— `cnc` — управляющий сервер злоумышленников;
— `phishing` — сетевой узел, связанный с фишингом;
— `download` — сетевой узел, связанный с загрузкой вредоносного ПО;
— `upload` — сетевой узел, связанный с эксфильтрацией данных.

4.3. Перечень атрибутов индикаторов компрометации

Ниже представлено описание имеющихся атрибутов для различных типов индикаторов компрометации.

В этом разделе

4.3.1. File и URL

Таблица 2. File и URL

Атрибут	Тип (формат)	Описание
`normalized_score`	Integer	Репутация объекта на момент выгрузки. От 0 до 100, где 100 — вредоносный, 0 — безопасный
`verdict`	String	Результат проверки. Возможные значения: `suspicious`, `clean`, `malicious`, `whitelisted`, `torrent_tracker`, `sinkhole`, `parking`, `public_dns_server`, `port_scanner`, `dyndns`, `cloud`, `stun`, `tor_node`, `crawler`, `cdn`, `ad_server`, `crl_ocsp`, `free_email`, `vpn_gate`, `ip_to_domain`, `free_proxy`
`timestamps`	Object	Временные метки
`timestamps → first_seen`	String (date-time)	Дата и время первого упоминания объекта
`timestamps → last_seen`	String (date-time)	Дата и время последнего упоминания объекта
`malware_class`	Array of strings	Классы вредоносного ПО, к которым относится файл
`malware_family`	Array of strings	Семейства вредоносного ПО, к которым относится файл
`malware_group`	Array of strings	Файл используется злоумышленниками

Атрибут	Тип (формат)	Описание
malware_campaign	Array of strings	Файл замечен во вредоносных кампаниях
severity	String	Потенциальный ущерб — возможное негативное влияние объекта на инфраструктуру организации. Возможные значения: — High — большой; — Medium — средний; — Low — малый; — None — неизвестен
is_apt	Boolean	Объект связан с активностью APT-группировок
relations	Array of objects	Информация о связях объекта с другими объектами
relations → target_type	String	Объект — цель связи. Возможные значения: IP, DOMAIN, FILE, URL, IP_RANGE
relations → type	String	Тип связи. Возможные значения: none, dropped_file, ip_resolved, called_ip, called_domain, called_url, downloaded_file, subdomain, ip_range, url_parent_domain, url_parent_ip, url_resolved, ptr_resolve, spf_domain
relations → key	String	Ключевой атрибут объекта — цели связи
relations → direction	String	Направление связи. Возможные значения: NONE, SOURCE, RECEIVER
av_verdicts	Array of strings	Результат проверки файла средствами антивирусной защиты

Атрибут	Тип (формат)	Описание
tags	Array of strings	Метки

4.3.2. IPaddress

Таблица 3. IPaddress

Атрибут	Тип (формат)	Описание
normalized_score	Integer	Репутация объекта на момент выгрузки. От 0 до 100, где 100 — вредоносный, 0 — безопасный
verdict	String	Результат проверки. Возможные значения: suspicious, clean, malicious, whitelisted, torrent_tracker, sinkhole, parking, public_dns_server, port_scanner, dyndns, cloud, stun, tor_node, crawler, cdn, ad_server, crl_ocsp, free_email, vpn_gate, ip_to_domain, free_proxy
timestamps	Object	Временные метки
timestamps → first_seen	String (date-time)	Дата и время первого упоминания объекта
timestamps → last_seen	String (date-time)	Дата и время последнего упоминания объекта
malware_class	Array of strings	Классы вредоносного ПО, к которым относится файл
malware_family	Array of strings	Семейства вредоносного ПО, к которым относится файл
malware_group	Array of strings	Файл используется злоумышленниками
malware_campaign	Array of strings	Файл замечен во вредоносных кампаниях

Атрибут	Тип (формат)	Описание
severity	String	Потенциальный ущерб — возможное негативное влияние объекта на инфраструктуру организации. Возможные значения: — High — большой; — Medium — средний; — Low — малый; — None — неизвестен
role	Array of strings	Роли узла в сети. Возможные значения атрибута: unknown, cnc, phishing, download, upload
is_apt	Boolean	Объект связан с активностью APT-группировок
geo	Object	Географические данные
geo → country_iso	String	Двухбуквенный код страны согласно ISO 3166-1
geo → city	String	Название города
geo → db_updated_at	String (date-time)	Дата и время обновления информации о геолокации
geo → country	String	Название страны
relations	Array of objects	Информация о связях объекта с другими объектами
relations → target_type	String	Объект — цель связи. Возможные значения: IP, DOMAIN, FILE, URL, IP_RANGE
relations → type	String	Тип связи. Возможные значения: none, dropped_file, ip_resolved, called_ip, called_domain, called_url, downloaded_file, subdomain, ip_range, url_parent_domain,

Атрибут	Тип (формат)	Описание
		`url_parent_ip`, `url_resolved`, `ptr_resolve`, `spf_domain`
`relations → key`	String	Ключевой атрибут объекта — цели связи
`relations → direction`	String	Направление связи. Возможные значения: `NONE`, `SOURCE`, `RECEIVER`
`av_verdicts`	Array of strings	Результат проверки файла средствами антивирусной защиты
`tags`	Array of strings	Метки

4.3.3. DomainName

Таблица 4. DomainName

Атрибут	Тип (формат)	Описание
`normalized_score`	Integer	Репутация объекта на момент выгрузки. От 0 до 100, где 100 — вредоносный, 0 — безопасный
`verdict`	String	Результат проверки. Возможные значения: `suspicious`, `clean`, `malicious`, `whitelisted`, `torrent_tracker`, `sinkhole`, `parking`, `public_dns_server`, `port_scanner`, `dyndns`, `cloud`, `stun`, `tor_node`, `crawler`, `cdn`, `ad_server`, `crl_ocsp`, `free_email`, `vpn_gate`, `ip_to_domain`, `free_proxy`
`timestamps`	Object	Временные метки
`timestamps → first_seen`	String (date-time)	Дата и время первого упоминания объекта
`timestamps → last_seen`	String (date-time)	Дата и время последнего упоминания объекта
`malware_class`	Array of strings	Классы вредоносного ПО, к которым относится файл

Атрибут	Тип (формат)	Описание
malware_family	Array of strings	Семейства вредоносного ПО, к которым относится файл
malware_group	Array of strings	Файл используется злоумышленниками
malware_campaign	Array of strings	Файл замечен во вредоносных кампаниях
severity	String	Потенциальный ущерб — возможное негативное влияние объекта на инфраструктуру организации. Возможные значения: — High — большой; — Medium — средний; — Low — малый; — None — неизвестен
role	Array of strings	Роли узла в сети. Возможные значения атрибута: unknown, cnc, phishing, download, upload
is_apt	Boolean	Объект связан с активностью APT-группировок
relations	Array of objects	Информация о связях объекта другими объектами
relations → target_type	String	Объект — цель связи. Возможные значения: IP, DOMAIN, FILE, URL, IP_RANGE
relations → type	String	Тип связи. Возможные значения: none, dropped_file, ip_resolved, called_ip, called_domain, called_url, downloaded_file, subdomain, ip_range, url_parent_domain, url_parent_ip, url_resolved, ptr_resolve, spf_domain
relations → key	String	Ключевой атрибут объекта — цели связи
relations → direction	String	Направление связи. Возможные значения: NONE, SOURCE, RECEIVER

Атрибут	Тип (формат)	Описание
av_verdicts	Array of strings	Результат проверки файла средствами антивирусной защиты
tags	Array of strings	Метки