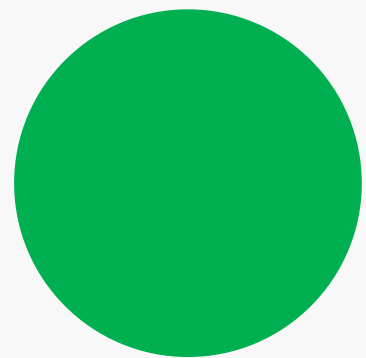
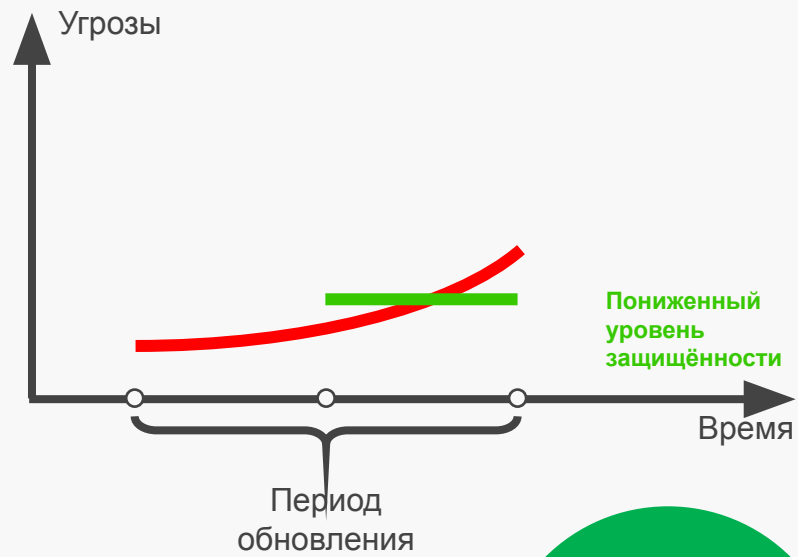


# Фантастический ТІ и где он обитает



# ПАРАДОКС ДОГОНЯЮЩЕГО ЧЕЛОВЕКА

- SIEM не успевает
- Правила непрофилированы
- Правила фолзят
- Правила устаревают
- Аналитики не успевают регулярно обновлять правила
- Open Source: БЗ корреляций уступают лидерам рынка



# ЧТО ТАКОЕ TI?

Знания о киберугрозах и злоумышленниках, позволяющие снизить либо ликвидировать риски в киберпространстве

Уровни TI

Стратегический

Операционный

Тактический

Технический



# ТЕХНИЧЕСКИЕ ИНДИКАТОРЫ



IP-адрес: 223.171.91.176

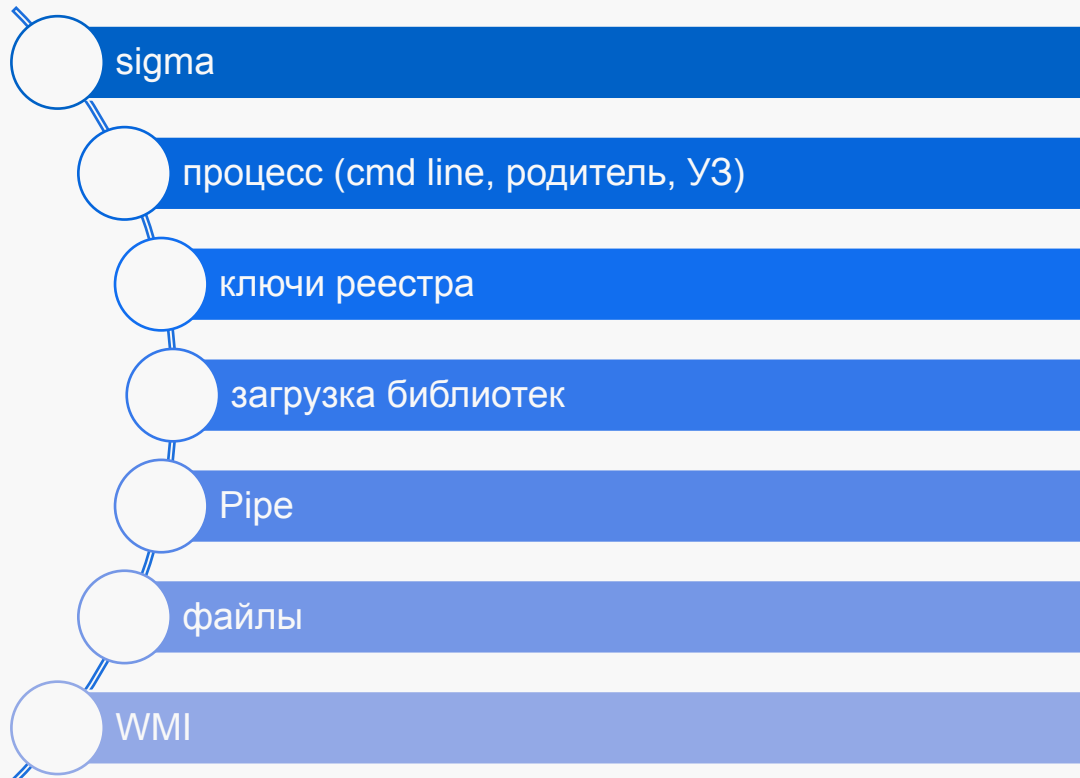
Домен: x2tesla.org

URL: <https://pastebin.com/raw/cxzpmqsz>

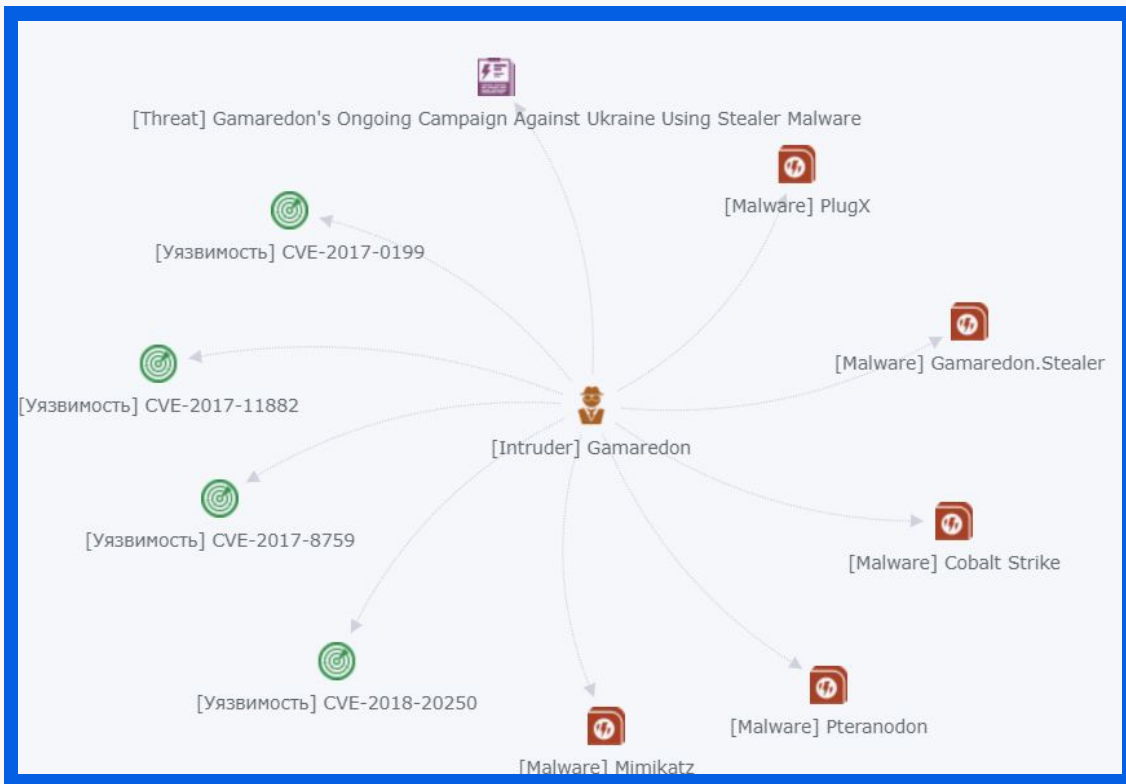
Хэш: d732b1e86fef628dd9a6496c25b63081392



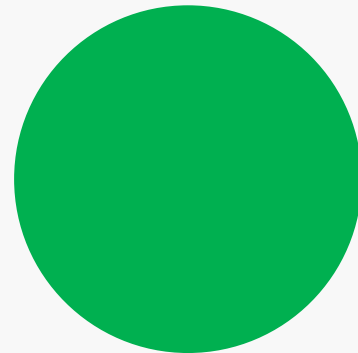
# ПОВЕДЕНЧЕСКИЕ ИНДИКАТОРЫ



# СТРАТЕГИЧЕСКИЕ ИНДИКАТОРЫ




- Злоумышленники
- Вредоносное ПО
- Угроза (вредоносная компания)



# ИСПОЛЬЗОВАНИЕ СОБРАННОЙ ИНФОРМАЦИИ

ИОС (Хэш)

Главная Аналитика Обнаружения Исходный JSON История

 Id: 8963155 Тэги: Bazon Shlem HyperBro [Выбрать](#)

Дата создания: 06.11.2022 16:09:29  
Статус: Активный

### Основная информация

**ace5920f0d22842eda2a20076870d463**

Хэш MD5: ace5920f0d22842eda2a20076870d463  
Хэш SHA1: 90cc4538742c279b3f1ea653e154e36e43f9cfa  
Хэш SHA256: 5cba27d29c89caf0c8a8d28b42a8f977f86c92c803d1e2c7386d60c0d864128  
SSDEEP: xk0RuAeeqJ+у8Kcs455mxUqIQ1Eeta2nFyjAHb06FGldR80Z1FDNUDvvc80A  
ОСК: xzTL55rEtadSpGnRb17UDv39pc6XtH5v

Категория: malware

Отрасль: Military

Страна: Belgium

Описание: IOC with tags: malware. Related threats: cobalt\_strike  
Дата первого обнаружения: 01.04.2022 00:00:00  
Дата последнего обнаружения: 13.10.2022 00:00:00  
MITRE ATT&CK: Steal or Forge Kerberos Tickets Exploitation for Defense Evasion

Техники ФСТЭК: T6.1 T6.8 Malware management

Добавлен в Active List: Нет

### Оценки

Оценка критичности: Высокая (70)

Оценка доверия: 80%

TLP: Amber

### Дополнительные детали индикатора

Наименование вредоносных файлов: sample.exe  
Тип вредоносных файлов: exe  
Размер вредоносных файлов (Байт): 722944  
Расширение:

### Стратегическая атрибуция

Вредоносное ПО: Cobalt Strike HyperBro

Злоумышленники: IronTiger

Угрозы: Irontiger aimed at a Middle Eastern country, U.S. and South East Asia

Связанные уязвимости: CVE-2011-3544 CVE-2021-40539



# ИСПОЛЬЗОВАНИЕ СОБРАННОЙ ИНФОРМАЦИИ

Ситуационная осведомленность

Идентификация инцидентов

Обнаружение технических ioc

Обнаружение аномальной активности

Ретро поиск новых ioc





# НАЙТИ СВОИ УНИКАЛЬНЫЕ ИСТОЧНИКИ ДАННЫХ

Rule Type	Strings Used	Example Detection
Regular	Program section of the PDB path	\\Release\loader.pdb
	Error messages	Target: Failed to load SAM functions.
	Persistence keywords	GoogleUpdateTaskMachineSystem
	Specific output strings	the file uploaded failed !
	Mutex values	LOADPREF_MUTEX
	Unique exports	FloodFix
	File references	C:\\ddd\\a1.txt
	Command combinations	-P /tmp && chmod +x /tmp/
Threat Intel Tracking	Username section of the PDB path	C:\\Users\\WMJI\\Desktop\\
	Author of malicious Office Docs	<cp:lastModifiedBy>Joohn</cp:lastModifiedBy>
	Email addresses	ahmed0med@outlook.com
	C2 server addresses	link.angellroofing.com
	Special keywords	Backsnarf_AB25
	Attacker vices	[base64 encoded "\$god = " variable]
	Developer fingerprint	Coded by z668
Method Detection	Special form of invocation	/RunProgram="hidcon:[a-zA-Z]{1,16}.cmd/
	Special form of obfuscation	c\` & \r\` & \i\` & \p\` & \t
	Special form of evasion	certutil -urlcache -split -f http
	Suspicious form of encoding	4D5A9000030000004000000FFFF0000B8000000
	Suspicious size	[big LNK files] uint16(0) == 0x004c and filesize > 200KB
	Suspicious combination	[Copyright is Microsoft Windows and SFX RAR]
	Persistence method	/\\Users\\Public\\[a-zA-Z]{1,16}.exe/
	Exploit code keywords	[+] Shellcode
	Usual suspicious exports	ReflectiveLoader

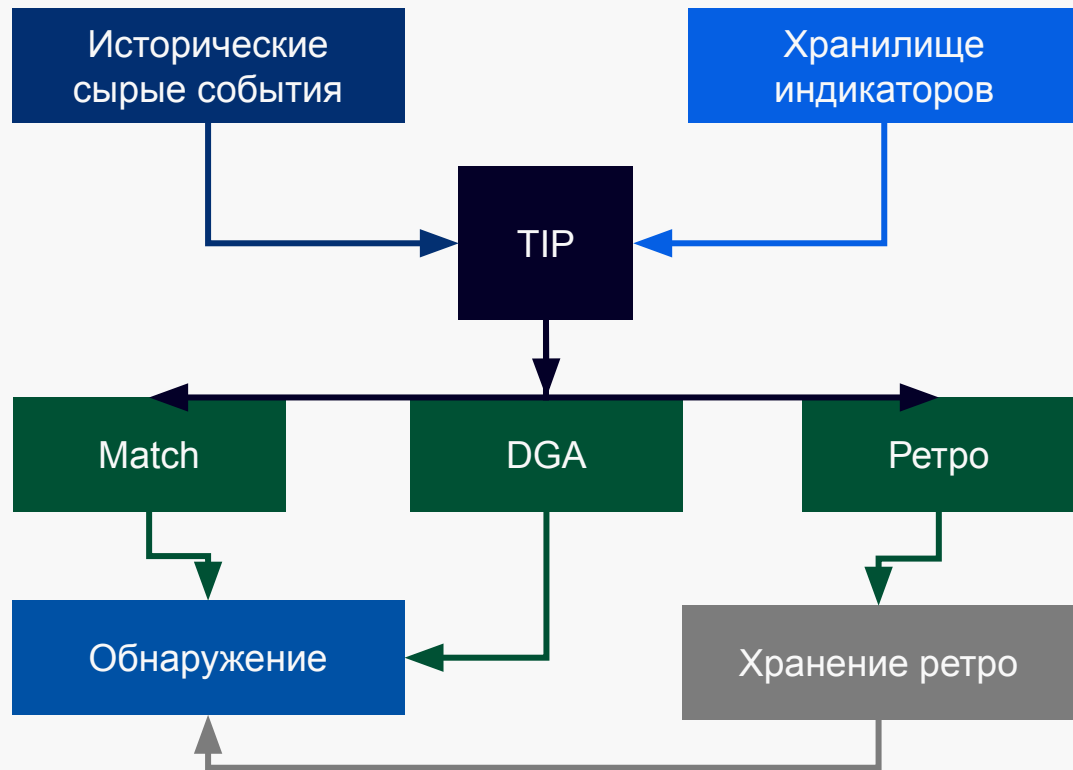
На основе своих инцидентов

Типы отраслевых инцидентов

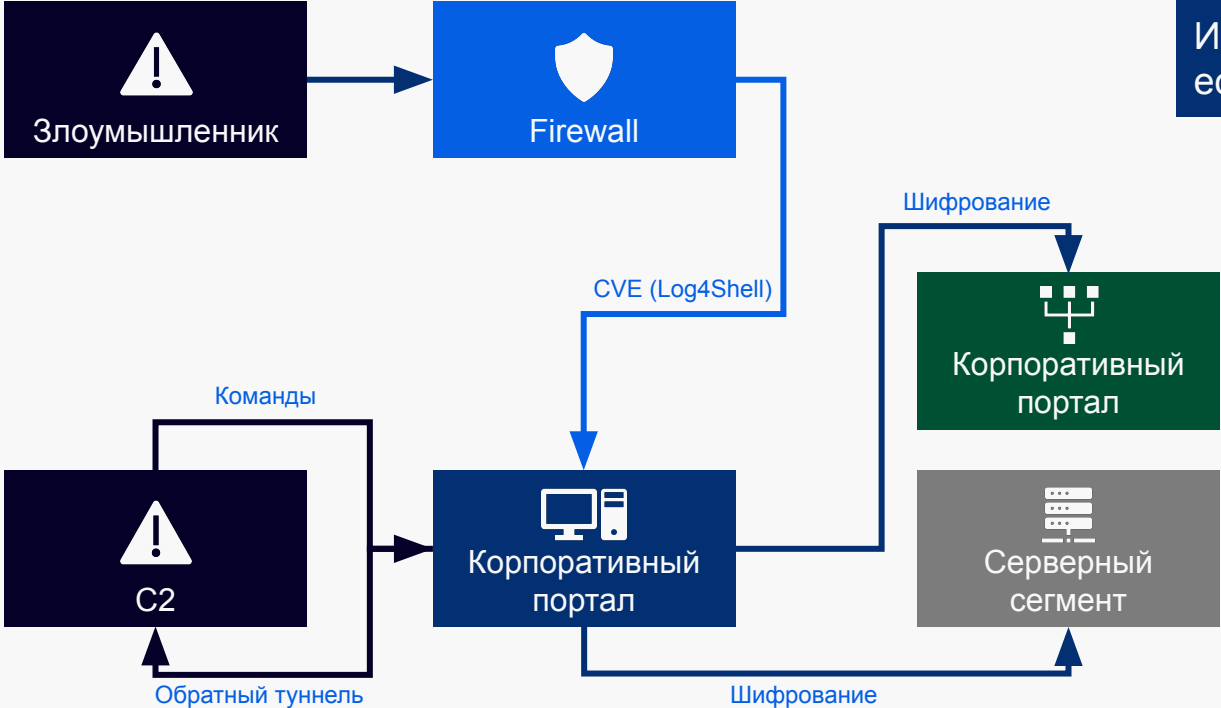
Гибкость подключаемых данных



# TI ДЛЯ ГЕНЕРАЦИИ ИНЦИДЕНТОВ

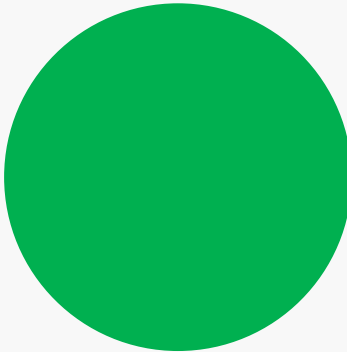


# ПРИМЕР РЕТРО-АНАЛИЗА ИНЦИДЕНТА И ОБОГОЩЕНИЯ

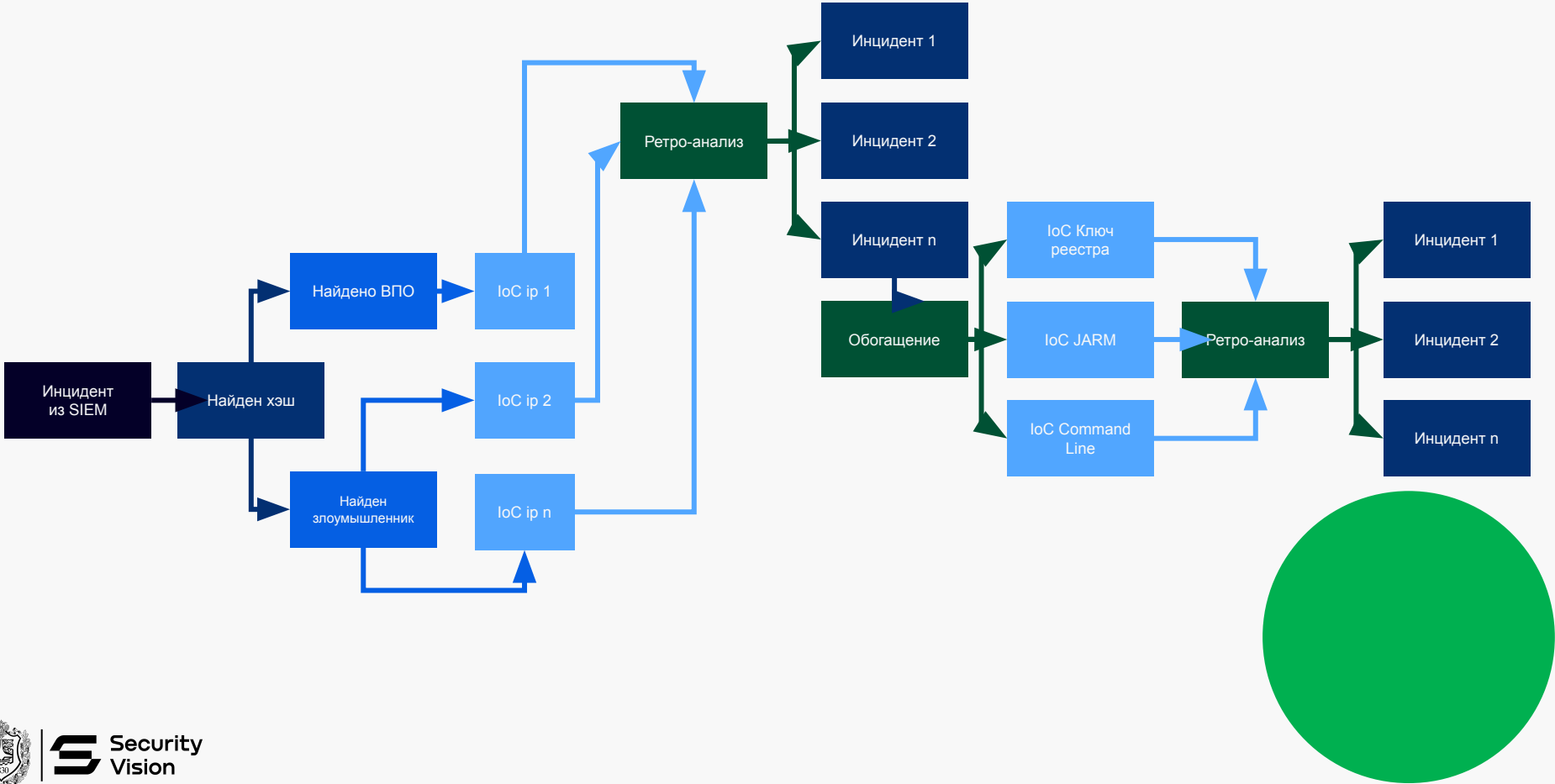


Инциденты лишены контекста если:

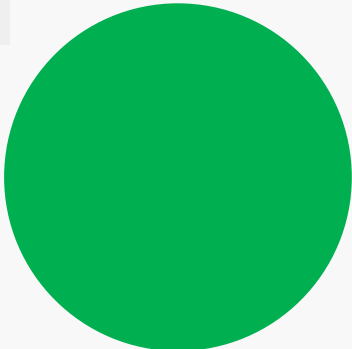
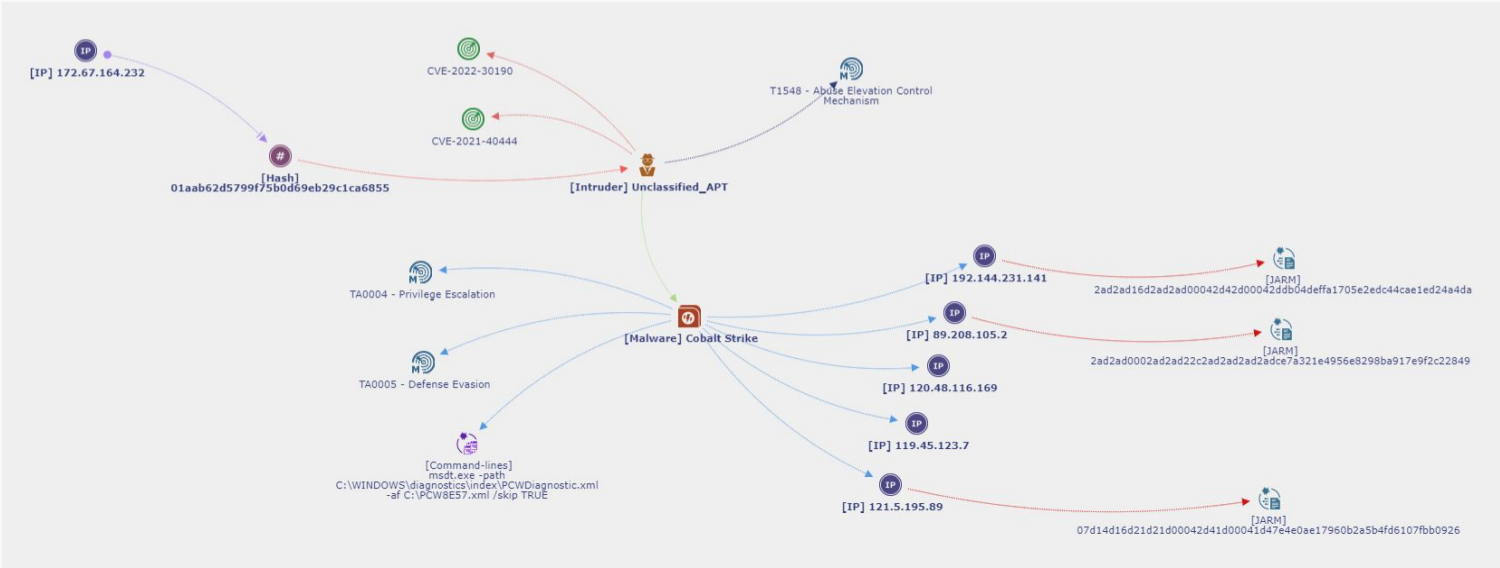
- антивирус, то это хэш
- письмо, то отправитель
- атакующий сервер, то IP



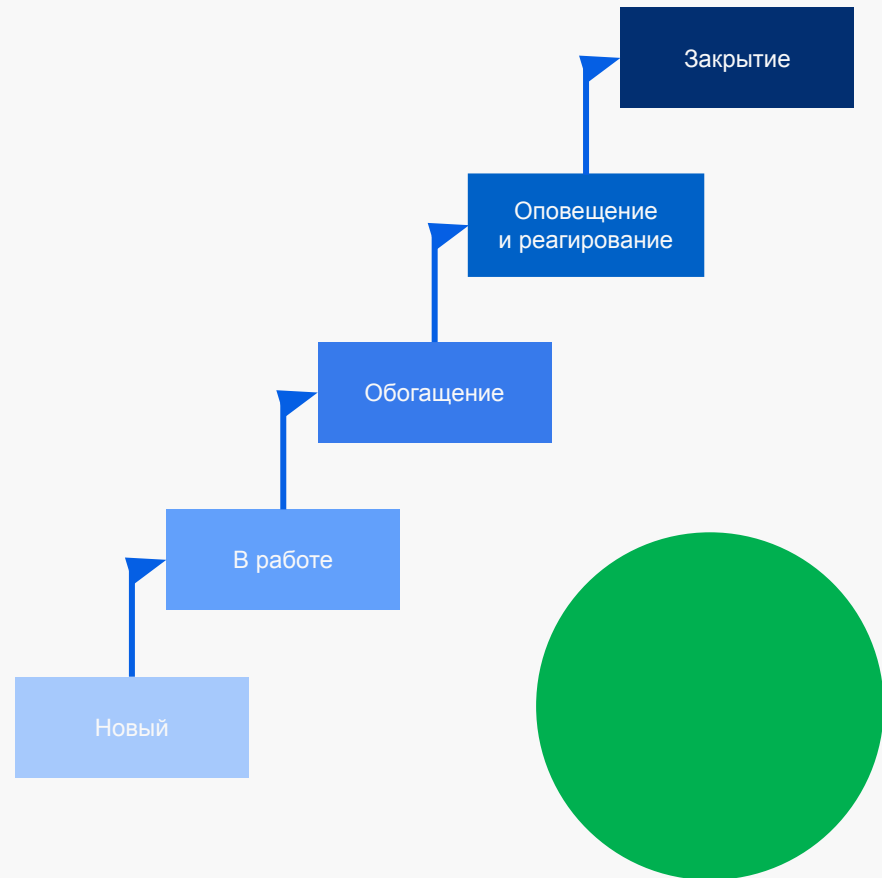
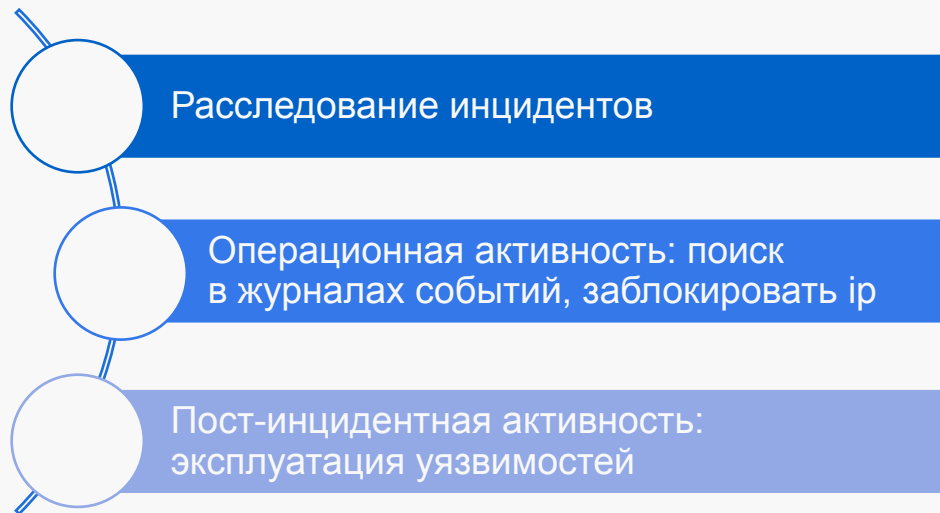
# РАССЛЕДОВАНИЕ ИНЦИДЕНТА



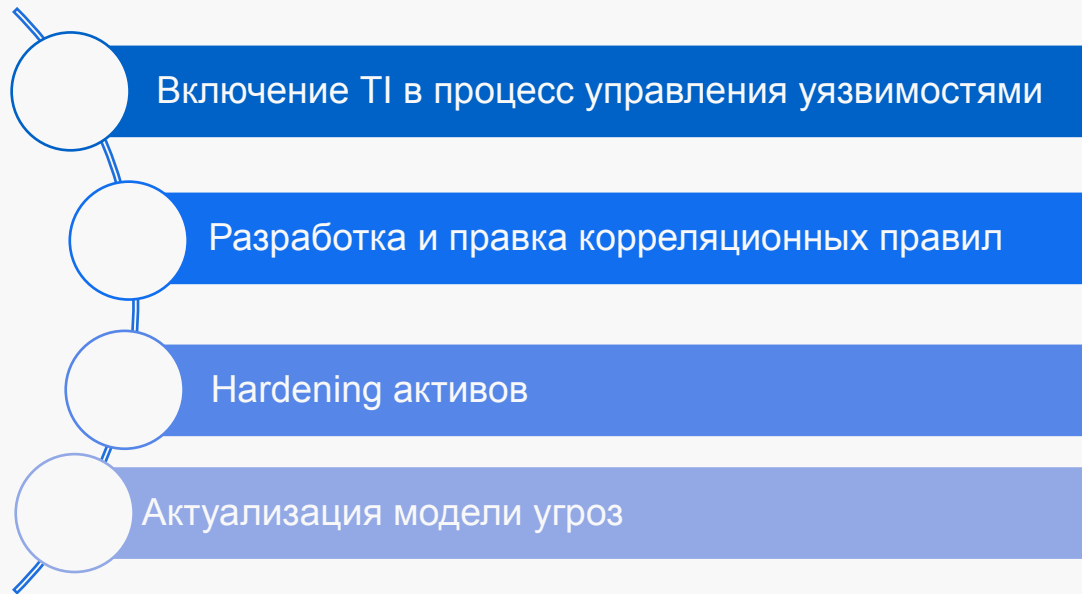
# ГРАФ СВЯЗЕЙ МЕТА-ИНЦИДЕНТА



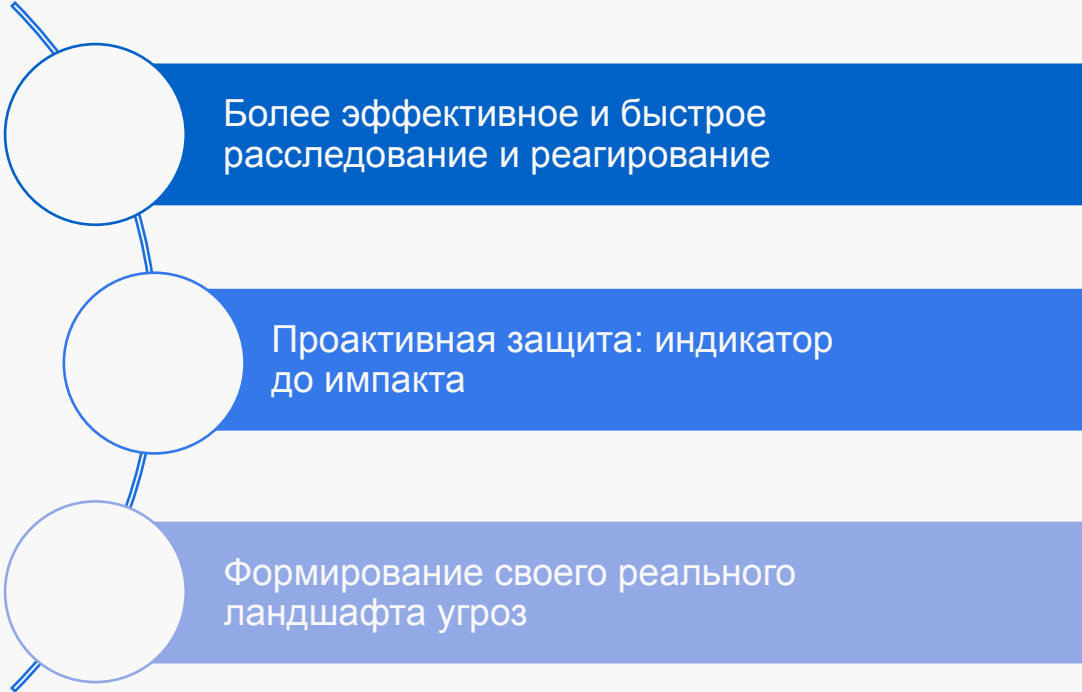
# ЭТАПЫ РАБОТЫ С ИНЦИДЕНТОМ



# ИСТОЧНИК ВДОХНОВЕНИЯ В ПОСЛЕДУЮЩИХ АКТИВНОСТЯХ



# ВЫВОДЫ:



Более эффективное и быстрое расследование и реагирование

Проактивная защита: индикатор до импакта

Формирование своего реального ландшафта угроз

