CTRLHACK

BAS нужен «полюBAS»

Система защиты

Средства защиты

Периметровые СЗИ, защита почты, антивирус, EDR, DLP

Анализ уязвимостей

Сканеры, пентесты

SOC

SIEM, аналитики, SOAR, команда реагирования

Ожидание и реальность

Система защиты должна обеспечивать определенный уровень защиты.

Должны проходить только атаки с использованием новых уязвимостей и техник.

Но на практике ситуация иная...

Примеры атак

18190 IcedID Macro Ends in Nokoyawa Ransomware		
	Tools	Technique
Initial Access		T1566.001 Phishing: Spearphishing Attachment
Execution	Microsoft Office Excel S0483 IcedID	T1204.002 User Execution: Malicious file Command and Scripting Interpreter: Windows Command Shell - T1059.003 T1059.004 Command and Scripting Interpreter: PowerShell T1059.005 Command and Scripting Interpreter: Visual Basic T1047 Windows Management Instrumentation
Persistence	S0483 IcedID	T1053.005 Scheduled Task/Job: Scheduled Task
Privilege Escalation	S0154 Cobalt Strike	T1134.001 Access Token Manipulation: Token Impersonation/Theft T1055 Process Injection
Defense Evasion		T1036.003 Masquerading: Rename System Utilities T1070.004 Indicator Removal: File Deletion T1218.011 System Binary Proxy Execution: Rundll32 T1078 Valid Accounts
Credential Access		T1552.001 Unsecured Credentials: Credentials in files T1003.001 OS Credential Dumping: LSASS Memory
Discovery	S0552 AdFind S0099 Arp Chcp Adget S0359 Nltest S0039 Net S0097 Ping S0096 Systeminfo S0483 IcedID S0154 Cobalt Strike	T1087.001 Account Discovery: Local Account T1087.002 Account Discovery: Domain Account T1083 File and Directory Discovery T1018 Remote System Discovery T1016 System Network Configuration Discovery T1482 Domain Trust Discovery
Lateral Movement	S0029 PsExec	T1021.001 Remote Services: Remote Desktop Protocol T1021.002 Remote Services: SMB/Windows Admin Shares T1021.006 Remote Services: Windows Remote Management
Collection	7 zip	T1560.001 Archive Collected Data: Archive via Utility
Command and Control	S0483 IcedID S0154 Cobalt Strike BackConnect VNC	T1071.001 Application Layer Protocol: Web Protocols T1105 Ingress Tool Transfer T1102 Web Service T1219 Remote Access Software
Exfiltration		T1041 Exfiltration Over C2 Channel
Impact	Nokoyawa Ransomware S0029 PsExec	T1486 Data Encrypted for Impact

- **Execution** — T1047 Windows Management Instrumentation
- **Persistence** — T1053.005 Scheduled Task/Job: Scheduled Task
- **Credential Access** — T1003.001 OS Credential Dumping: LSASS Memory
- **Lateral Movement** — Несколько техник с использованием утилиты PsExec

Что приводит к пропуску атак?

Система защиты работает не так, как ожидается

Средства защиты

Некорректно работающие СЗИ.
Исключения в правилах.
Отсутствие необходимых обновлений.
При этом далеко не все техники СЗИ могут заблокировать. Должны работать правила детектирования в SIEM.

SOC/SIEM

Отсутствие необходимых правил. Некорректная работа правил. Отсутствие необходимых событий или отключение сбора событий на определенной части инфраструктуры. Изменения в инфраструктуре. Время реагирования.

Атаки
и сканер уязвимостей

Сканер показывает только наличие определенных уязвимостей.
Но хакер использует уязвимости только на двух-трех стадиях атаки.
На остальных шагах уязвимости не используются.

Техники на этих шагах можно проверить только с использованием BAS систем.

Примеры атак

18041#-Malicious ISO File Leads to Domain Wide Ransomware			
	Tools	Technique	Exploited Vulnerabilities
Initial Access		T1566.001 Phishing: Spearphishing Attachment	
Execution	IcedID Cobalt Strike	T1059.001 Command and Scripting Interpreter: PowerShell T1059.003 Command and Scripting Interpreter: Windows Command Shell T1204.002 User Execution: Malicious File T1569.002 System Services: Service Execution T1047 Windows Management Instrumentation	
Persistence	IcedID	T1053.005 Scheduled Task/Job: Scheduled Task	
Privilege Escalation	Cobalt Strike — GetSystem	T1134.001 Access Token Manipulation: Token Impersonation/Theft T1068 Exploitation for Privilege Escalation	ZeroLogon CVE-2020-1472
Defense Evasion		T1562.001 Impair Defenses: Disable or Modify Tools T1218.010 System Binary Proxy Execution: Regsvr32 T1218.011 System Binary Proxy Execution: Rundll32 T1055 Process Injection T1553.005 Mark-of-the-Web Bypass	
Credential Access	Mimikatz ProcDump	T1003.001 OS Credential Dumping: LSASS Memory T1003.006 OS Credential Dumping: DCSync	
Discovery	IcedID — nltest, net, chcp, ipconfig, systeminfo Cobalt Strike — net, nslookup, Invoke-ShareFinder, Get-EventLog, Get-ADComputer, Custom PowerShell, Custom Batch Scripts, Adget, WMI Queries, dir RDP — Group Policy, Invoke-ShareFinder, Veeam Backup Console	T1482 Domain Trust Discovery T1082 System Information Discovery T1018 Remote System Discovery T1615 Group Policy Discovery T1614.001 System Location Discovery: System Language Discovery T1124 System Time Discovery T1135 Network Share Discovery T1087.002 Account Discovery: Domain Account T1083 File and Directory Discovery T1033 System Owner/User Discovery	
Lateral Movement	Cobalt Strike	T1021.001 Remote Services: Remote Desktop Protocol T1021.002 Remote Services: SMB/Windows Admin Shares T1021.006 Remote Services: Windows Remote Management T1570 Lateral Tool Transfer	
Collection	Local Files Text, TSV, CSV	T1074.001 Data Staged: Local Data Staging	
Command and Control	IcedID Cobalt Strike AnyDesk Atera Splashtop	T1071.001 Application Layer Protocol: Web Protocols	
Exfiltration	Rclone — Mega.io	T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage	
Impact	Quantum Ransomware net user	T1486 Data Encrypted for Impact T1531 Account Access Removal	

18190 IcedID Macro Ends in Nokoyawa Ransomware		
	Tools	Technique
Initial Access		T1566.001 Phishing: Spearphishing Attachment
Execution	Microsoft Office Excel S0483 IcedID	T1204.002 User Execution: Malicious file Command and Scripting Interpreter: Windows Command Shell – T1059.003 T1059.004 Command and Scripting Interpreter: PowerShell T1059.005 Command and Scripting Interpreter: Visual Basic T1047 Windows Management Instrumentation
Persistence	S0483 IcedID	T1053.005 Scheduled Task/Job: Scheduled Task
Privilege Escalation	S0154 Cobalt Strike	T1134.001 Access Token Manipulation: Token Impersonation/Theft T1055 Process Injection
Defense Evasion		T1036.003 Masquerading: Rename System Utilities T1070.004 Indicator Removal: File Deletion T1218.011 System Binary Proxy Execution: Rundll32 T1078 Valid Accounts
Credential Access		T1552.001 Unsecured Credentials: Credentials in files T1003.001 OS Credential Dumping: LSASS Memory
Discovery	S0552 AdFind S0099 Arp Chcp Adget S0359 Nltest S0039 Net S0097 Ping S0096 Systeminfo S0483 IcedID S0154 Cobalt Strike	T1087.001 Account Discovery: Local Account T1087.002 Account Discovery: Domain Account T1083 File and Directory Discovery T1018 Remote System Discovery T1016 System Network Configuration Discovery T1482 Domain Trust Discovery
Lateral Movement	S0029 PsExec	T1021.001 Remote Services: Remote Desktop Protocol T1021.002 Remote Services: SMB/Windows Admin Shares T1021.006 Remote Services: Windows Remote Management
Collection	7 zip	T1560.001 Archive Collected Data: Archive via Utility
Command and Control	S0483 IcedID S0154 Cobalt Strike BackConnect VNC	T1071.001 Application Layer Protocol: Web Protocols T1105 Ingress Tool Transfer T1102 Web Service T1219 Remote Access Software
Exfiltration		T1041 Exfiltration Over C2 Channel
Impact	Nokoyawa Ransomware S0029 PsExec	T1486 Data Encrypted for Impact

Атаки
и сканер уязвимостей

Используемые хакерами техники:

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 техник	10 техник	17 техник	12 техник	32 техники	14 техник	22 техники	9 техник	15 техник	16 техник	8 техник	13 техник

Уязвимости используются только на трех стадиях.

Сканер работает также только для некоторых техник на этих стадиях.

Breach and Attack Simulation BAS

Симуляция хакерских техник в инфраструктуре компании

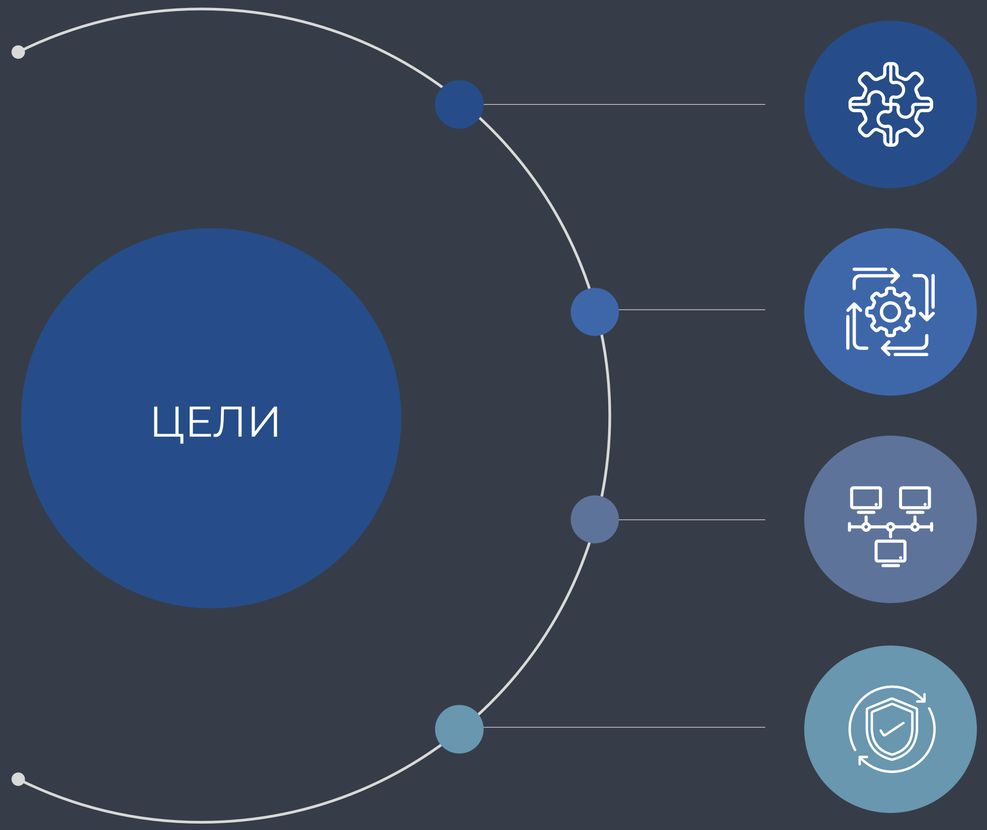
Имитируют действия хакеров в автоматическом режиме

Нацелены на проверку внутренней инфраструктуры

Позволяют построить процесс непрерывной оценки системы защиты

Системы класса BAS

Симуляция хакерских техник в инфраструктуре компании



Проверка работы средств защиты

Проверка покрытия правилами детектирования

Проверка всей инфраструктуры

Повышение эффективности детектирования

Примеры решений

Atomic Red Team

- Open Source
- Большой набор техник. Техники обновляются.
- Техники нужно проверять. Нельзя запускать без проверки.
- Нет возможности запуска по всей инфраструктуре. Все запуски выполняются вручную.
- Результаты нужно собирать вручную. Нет отчетов.
- Невозможно построить процесс.
- Возможно применять на небольших стендах для отработки правил детектирования.

https://atomicredteam.io/
https://github.com/redcanaryco/atomic-red-team

Примеры решений

CALDERA

- Open Source
- Много техник из Atomic. Техники обновляются.
- Техники также нужно проверять.
- Есть графический интерфейс и есть возможность автоматического запуска и централизованного сбора отчетов.
- Не для всех техник есть детальный отчет.
- Агент после перезагрузки машины или после сработки средств защиты приходится переустанавливать.

https://caldera.mitre.org/

https://github.com/mitre/caldera

CTRLHACK BAS FELIX

Проверка работы:

NGFW, антивируса, EDR,
песочницы и почтового антивируса,
правил детектирования в SIEM.

СИМУЛЯЦИЯ ТЕХНИК

Пошаговая симуляция техник MITRE и сценариев первичного доступа на установленных в инфраструктуре агентах. **300 техник**.

ЗАДАЧИ

Проверка работы средств защиты, валидация правил детектирования в SIEM, контроль поступления событий безопасности, контроль процессов реагирования.

РЕЗУЛЬТАТ

Выявление проблем в системе защиты, и белых пятен в детектировании. Как результат повышение эффективности детектирования техник на **30-50%**.

Результаты работы CTRLHACK BAS FELIX

Проверка средств защиты

Отсутствие обновлений антивирусов, проблемы с EDR, пропуск вредоносного трафика на NGFW.

Детектирование техник

Выключенные правила, отсутствие правил, отсутствие событий, выключенный сбор событий на узлах.

Развитие SOC

Задержки в формировании карточки инцидентов.

Результаты работы

CTRLHACK BAS FELIX

01 **EDR:** техники Windows
обнаружено 60% техник,
заблокировано только 24%.

02 **SIEM:** техники Windows – детектирование от 30 до 70%,
техники Windows – детектирование менее 30%.

03 **Инциденты:** поднятие карточки – 15 мин, 6 часов.

Опыт использования CTRLHACK BAS FELIX

Валидация и развитие правил детектирования на уровне SOC.

Проверка корректности работы внедренных СЗИ.

Использование в сегменте АСУТП.

Настройка и контроль работы EDR.

Тестирование СЗИ в рамках пилотов.

Оценка дочерних организаций.

Не внедряйте новые СЗИ пока не поняли, что могут блокировать имеющиеся.

Симуляция поможет это понять.

01 Повышается эффективность существующих СЗИ

02 Появляется возможность постоянного развития правил SIEM

03 Снижаются требования к персоналу и трудозатраты

ООО «КОНТРОЛХАК»
+7 (495) 789 72 97
info@ctrlhack.ru

ПРИГЛАШАЕМ ВАС НА НАШ СТЕНД

СПАСИБО!

ВСЕГДА РАДЫ СОТРУДНИЧЕСТВУ