Примеры сценариев автоматизации пентеста

Валерий Филин
Технический директор

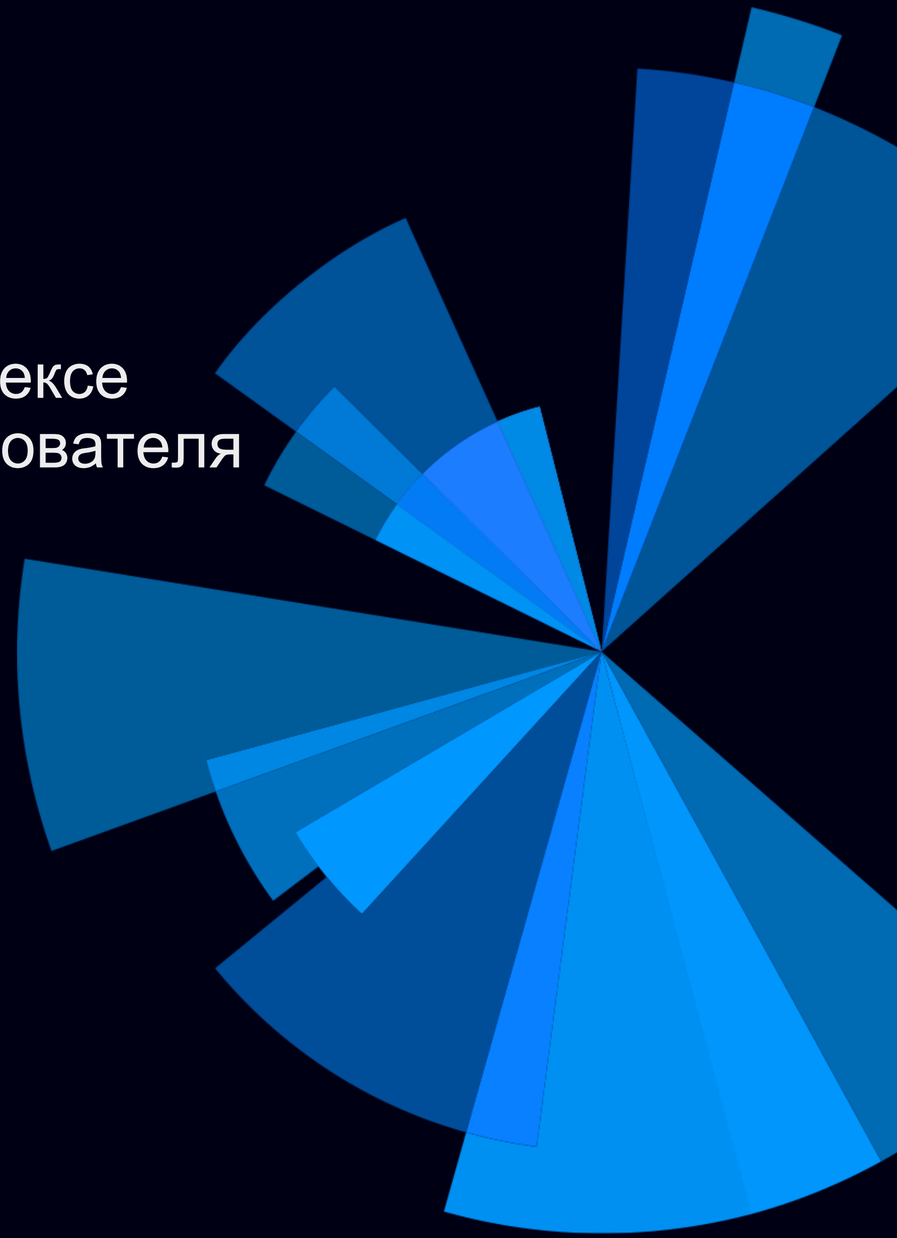
CITUM – экспертный дистрибьютор

Тестирование на проникновение

- Практическая оценка:
  - Конкретная сеть
  - Конкретные начальные условия
  - Конкретная цель
  - Активная эксплуатация
  - Подтвержденные векторы атак
  - Релевантные рекомендации

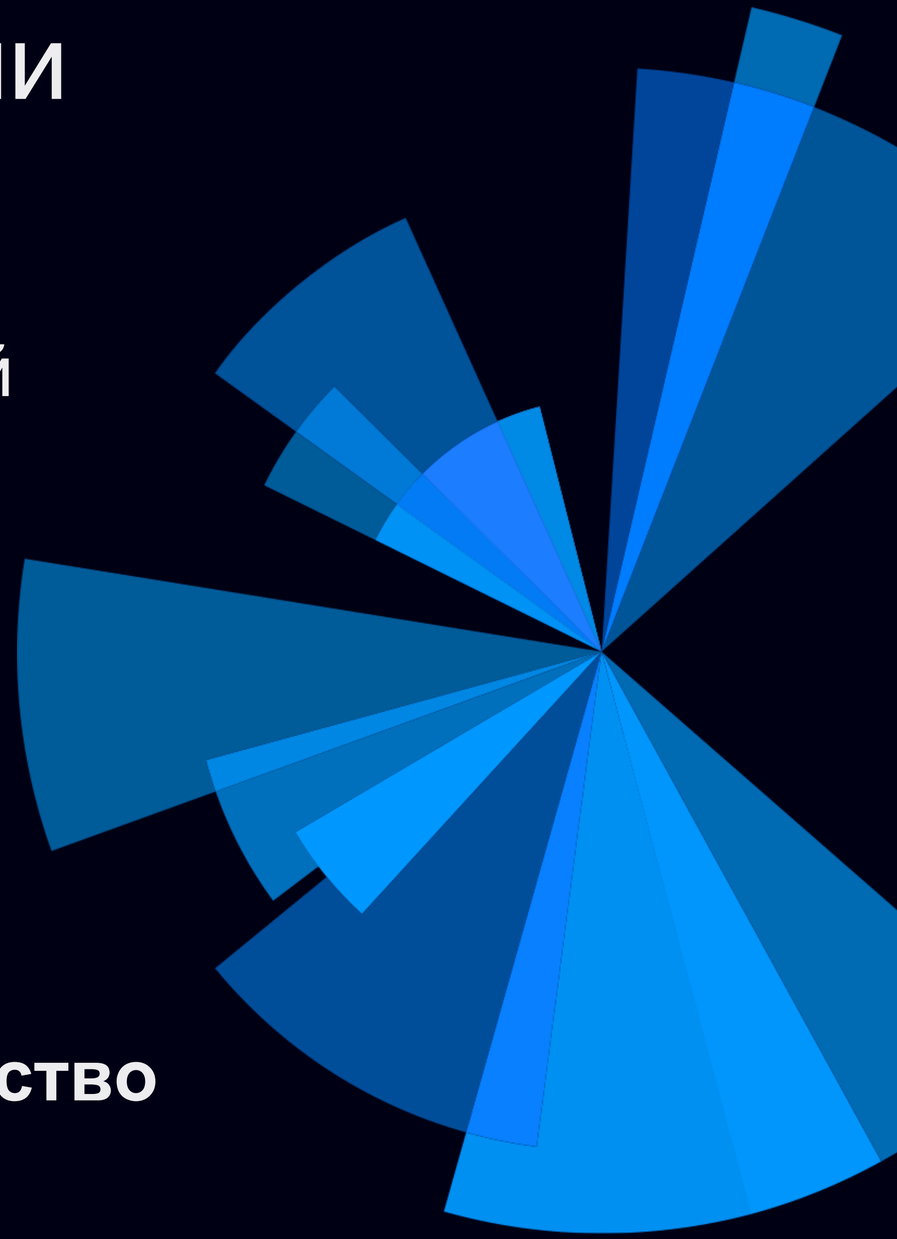
Ключевые бизнес-сценарии

- Что можно протестировать?
  - устойчивость сети к реальной атаке в комплексе
  - сценарий компрометации конкретного пользователя
  - безопасность ценных активов и данных
  - надежность доменных политик
  - качество управления привилегиями
  - безопасность ключевых сетевых настроек
  - эффективность средств защиты
  - эффективность процессов реагирования
  - классические CVE-уязвимости



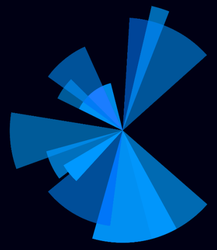
Преимущества автоматизации

- Высокая скорость анализа
- Мгновенная проверка после исправлений
- Непрерывная проверка защищенности
- Произвольное масштабирование
- Экономия человеческого ресурса
- Целостный результат оценки
- Неразглашение информации



Алгоритмы - машине, человеку – творчество

Решение



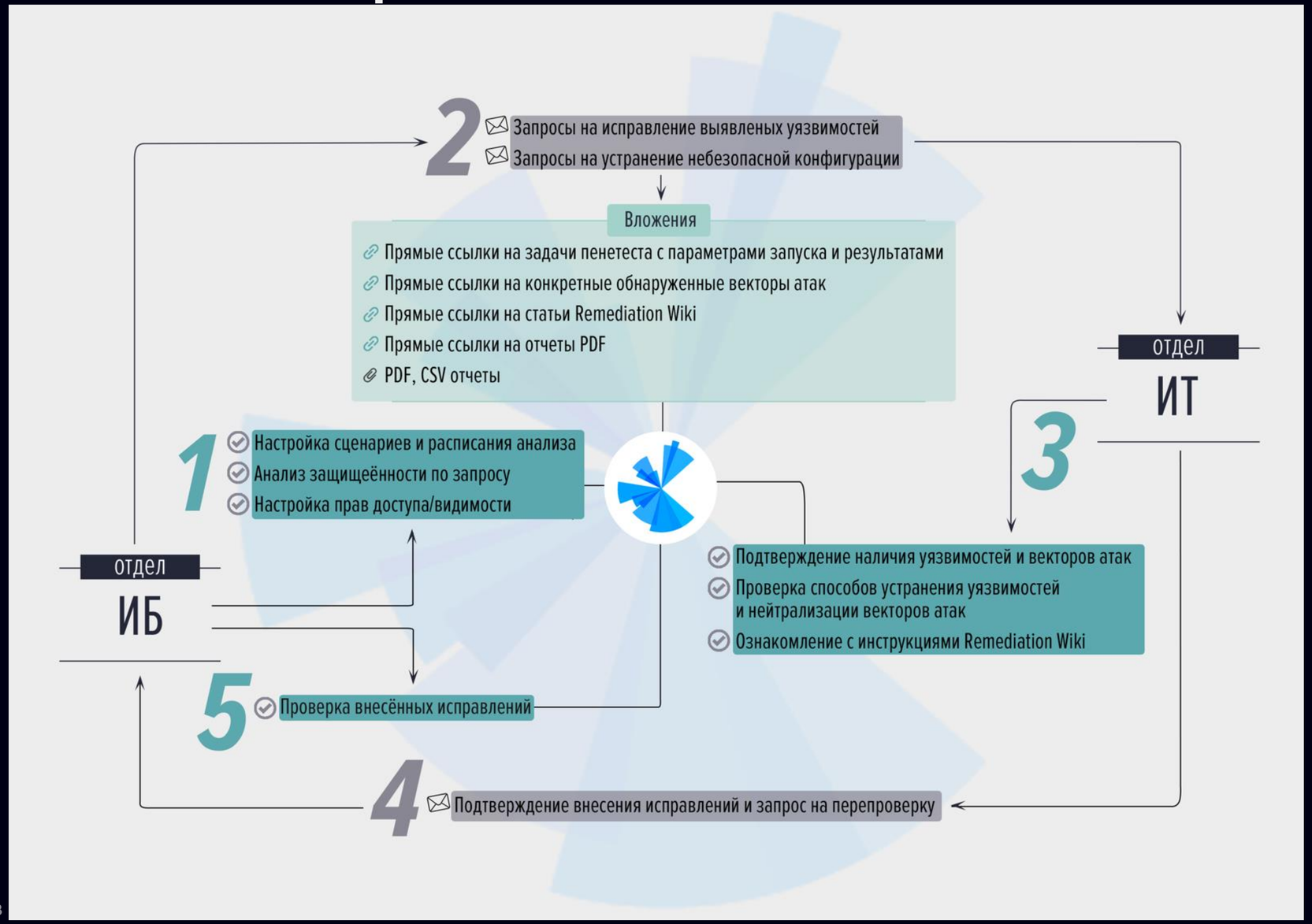
PenTera™ /

By Pcysys

Первая в мире платформа
автоматизации тестов на проникновение

Интеграция в бизнес процессы

- PenTera – ядро коммуникаций
- Простой запуск теста
- Релевантные рекомендации
- Наглядное обоснование исправления для ИТ
- Подробные инструкции
- Мгновенная проверка исправления

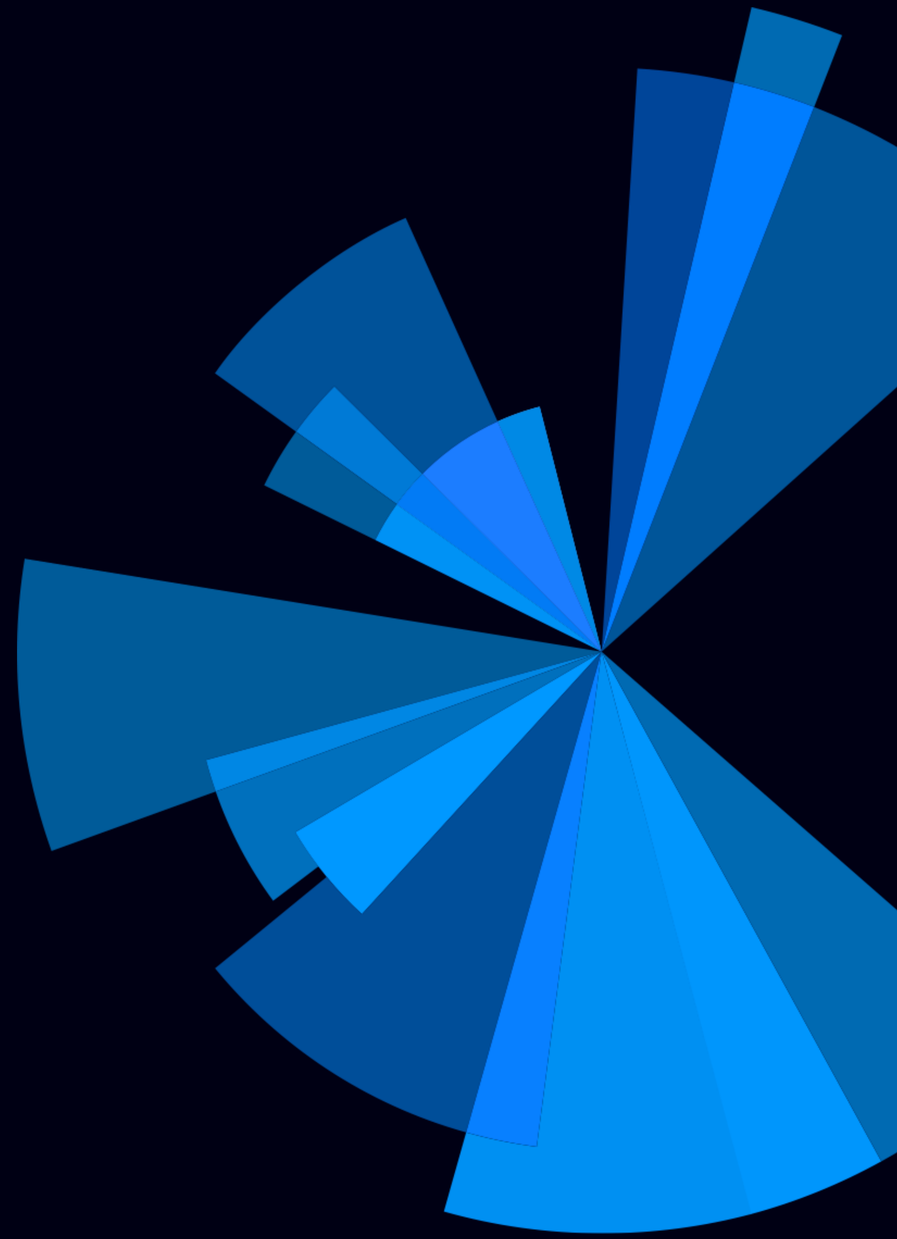


Примеры сценариев

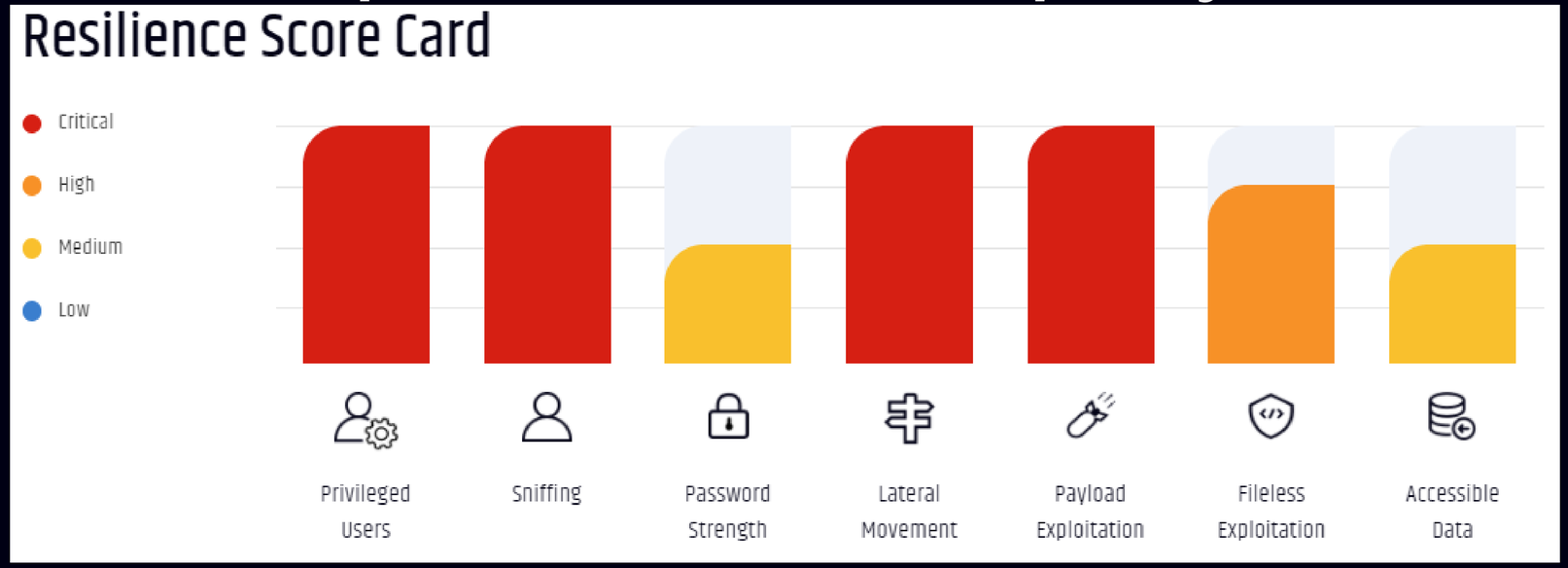
- Тестирование в режиме «черного ящика»
- Тестирование в режиме «серого ящика»
- Контроль соблюдения парольной политики
- Тестирование средств защиты на местах
- Тестирование и оптимизация SOC

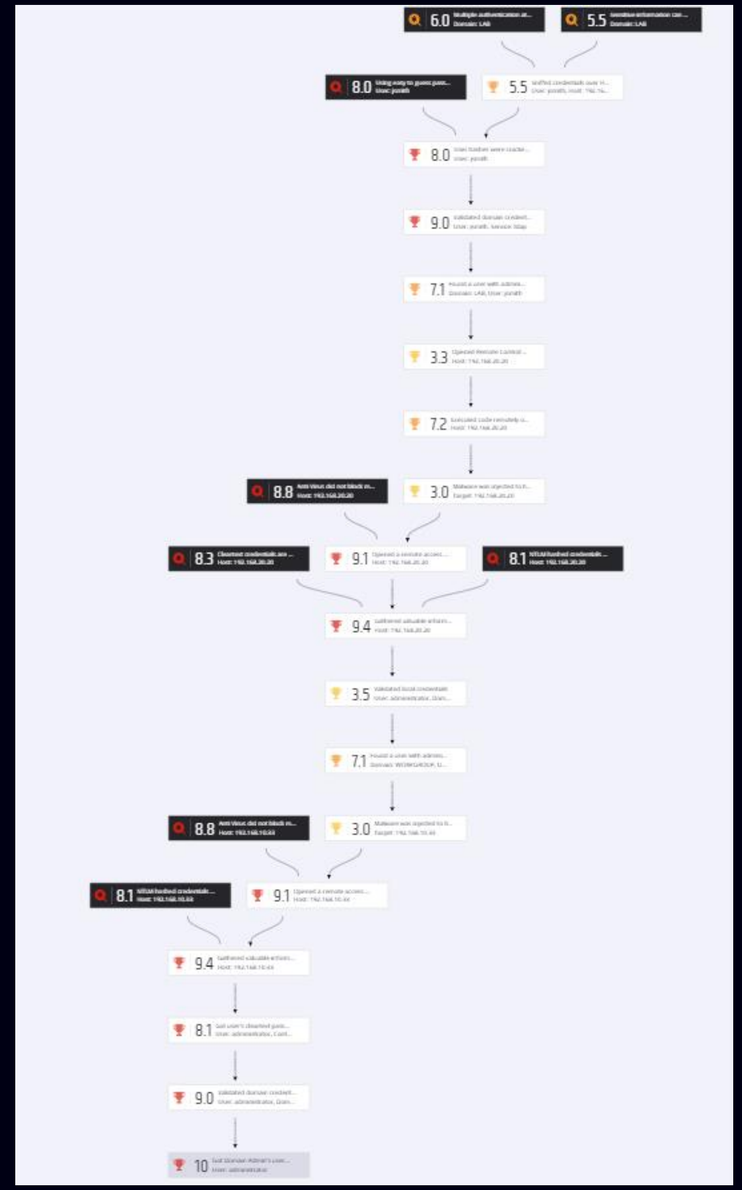
«Черный ящик»

- Подготовка (5 минут):
  - Определить начальную точку атаки
  - Определить масштабы теста
  - Определить уровень скрытности
  - Настроить задачу
- Тестирование (автоматически, 2 дня)



«Черный ящик» - результат

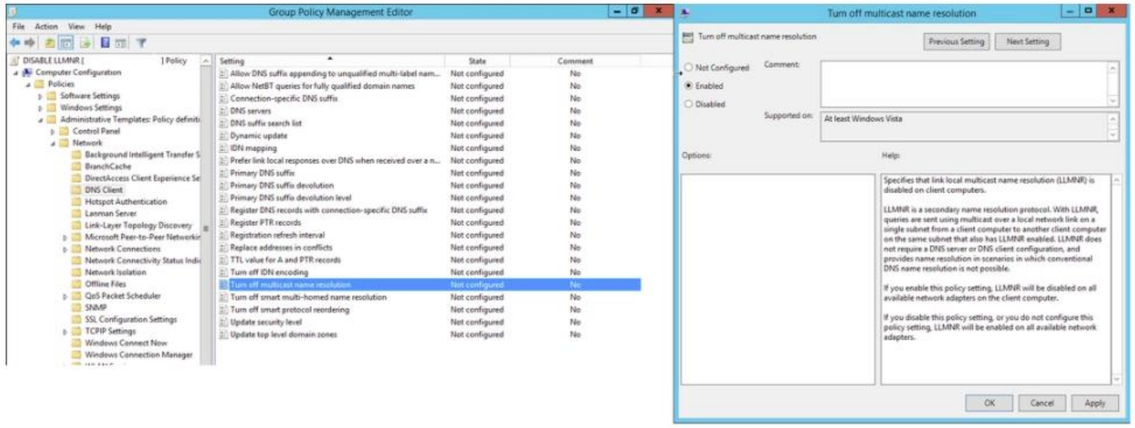




Recommendations

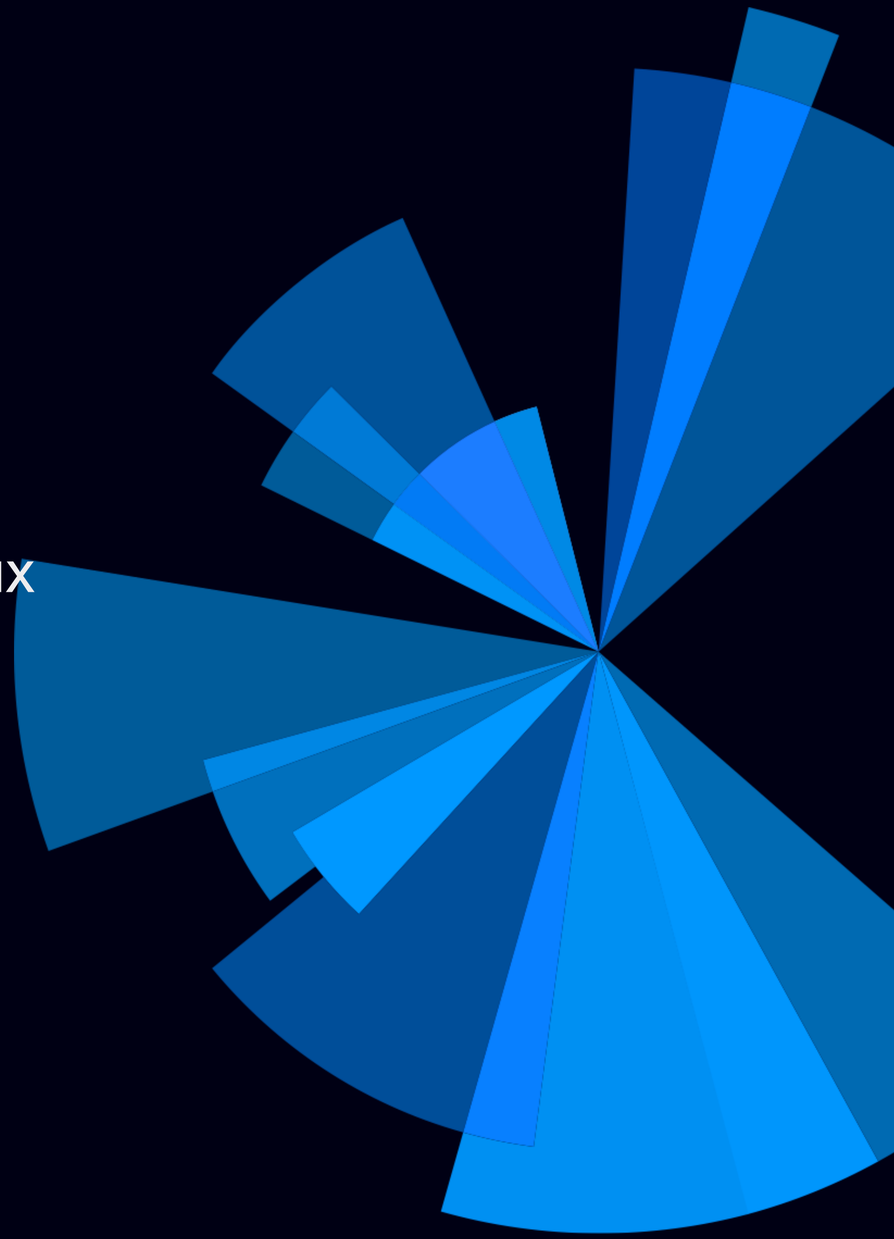
It is recommended to disable these protocols, which can be done as follows:

- **LLMNR** – can be disabled using GPO
  - Create a new GPO record for all computers in the environment
  - Navigate to "Local Computer Policy / Computer Configuration / Administrative Templates / Network / DNS Client"
  - Set "**Turn Off Multicast Name Resolution**" to "**Enabled**"



«Серый ящик»

- Подготовка (20 минут):
  - Определить начальную точку
  - Определить масштабы теста
  - Определить уровень скрытности
  - Определить ключевые слова для поиска данных
  - Подготовить учетные данные пользователя
  - Настроить задачу
- Тестирование (автоматически, 2 дня)

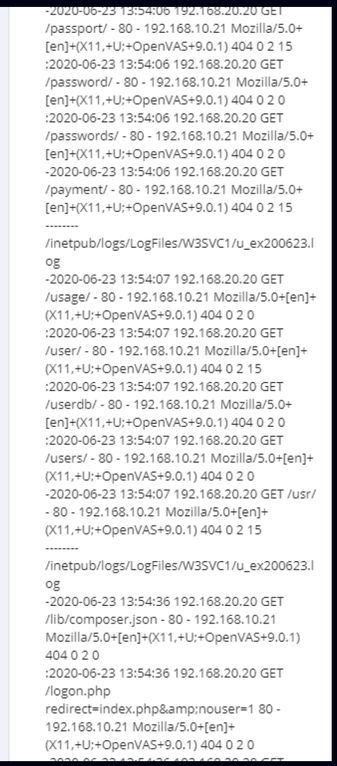


«Серый ящик» - результат

HASHED DOMAIN CREDENTIALS

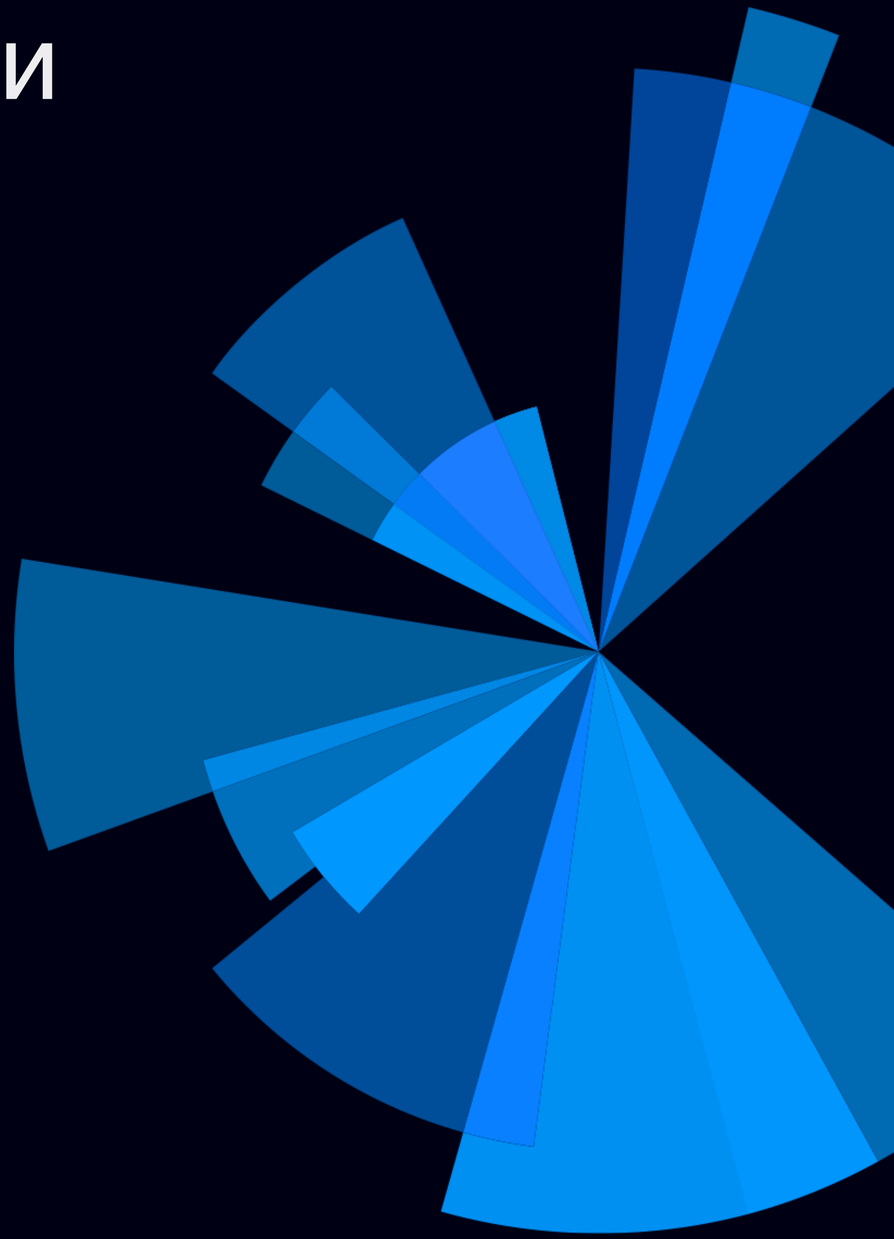
Username	Domain	Ntlm	Sha1
healthmailboxd4fb499	LAB	0a******	
healthmailboxe1c1f55	LAB	5e******	
healthmailboxfd0f8d1	LAB	2b******	
hp-office$	LAB	dd******	
ivanti$	LAB	1f******	
ivanti01$	LAB	48******	
jdoe	LAB	9b******	
jsmith	LAB	90******	
krbtgt	LAB	43******	

Rows per pa



Проверка парольной политики

- Подготовка (1 минута):
  - Выбрать нужный контроллер домена
  - Подготовить учетные данные пользователя
  - Настроить задачу
- Тестирование (автоматически, 2-3 дня)

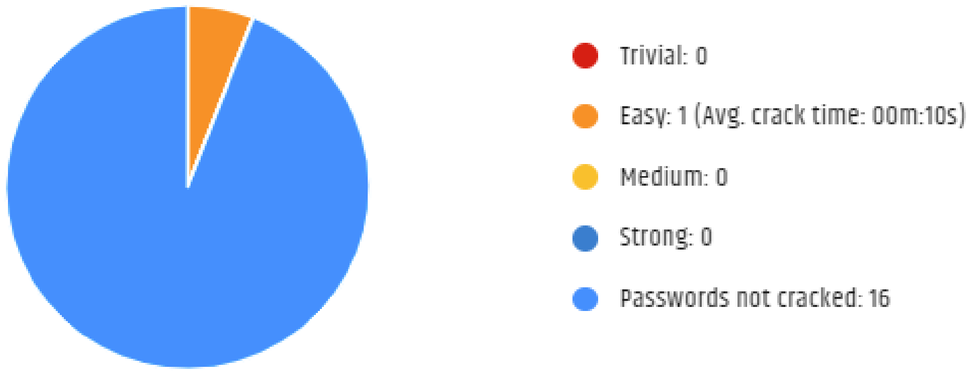


Проверка парольной политики - результат

PenTera™ Lab - Password Policy Sep 9th 2020

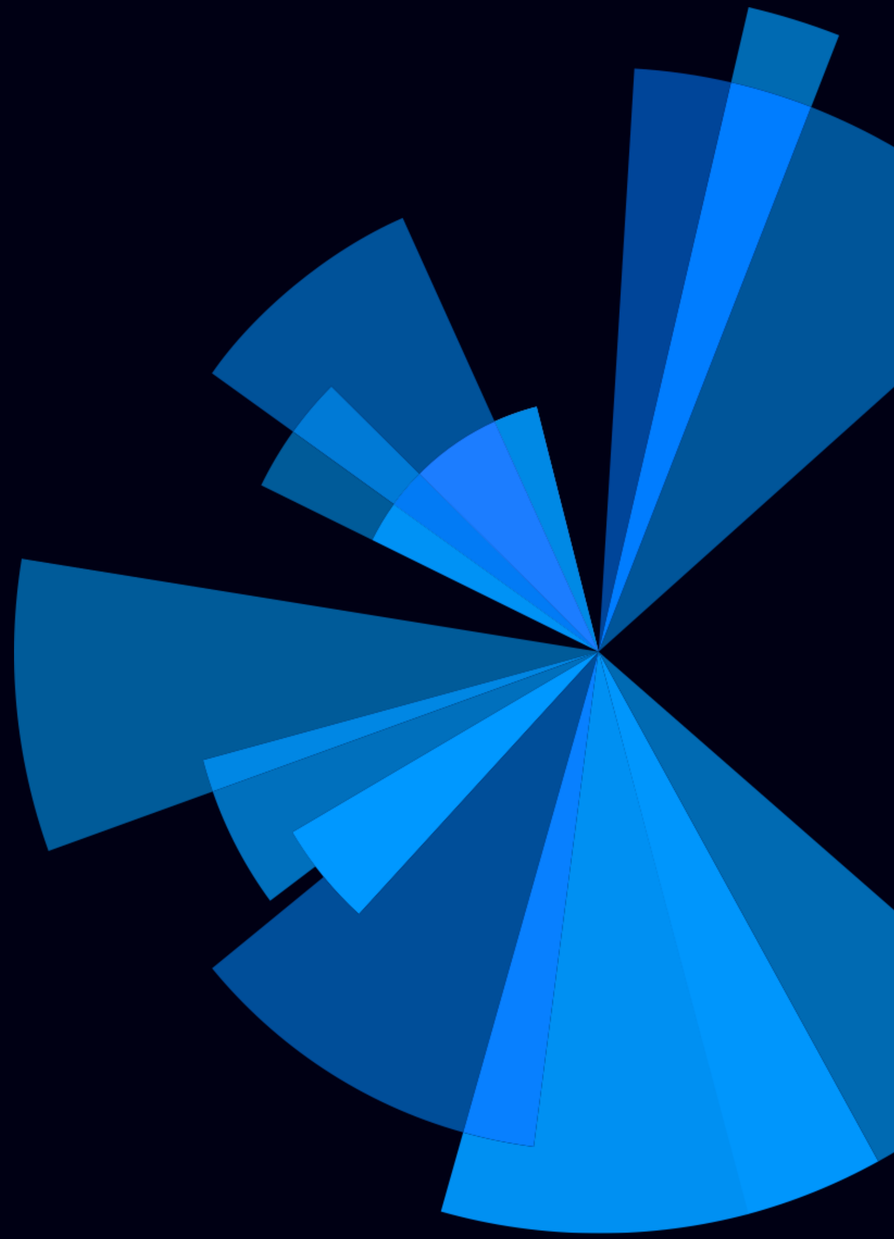
1 / 17

Password cracking



Проверка средств защиты

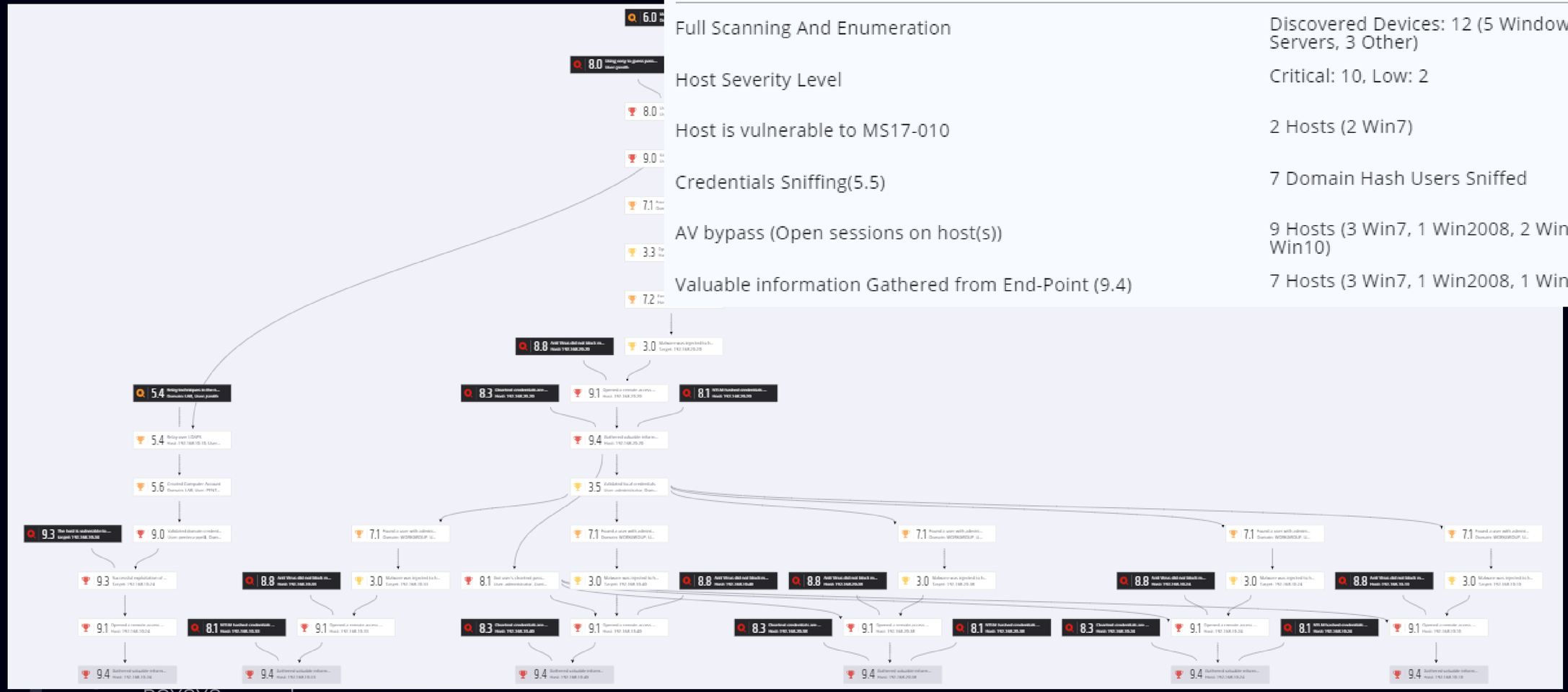
- Подготовка (5 минут):
  - Настроить интеграцию с SIEM
  - Определить масштабы теста
  - Подготовить учетные данные пользователя
  - Настроить задачу
- Тестирование (автоматически, 2 дня)



Проверка средств защиты - результат

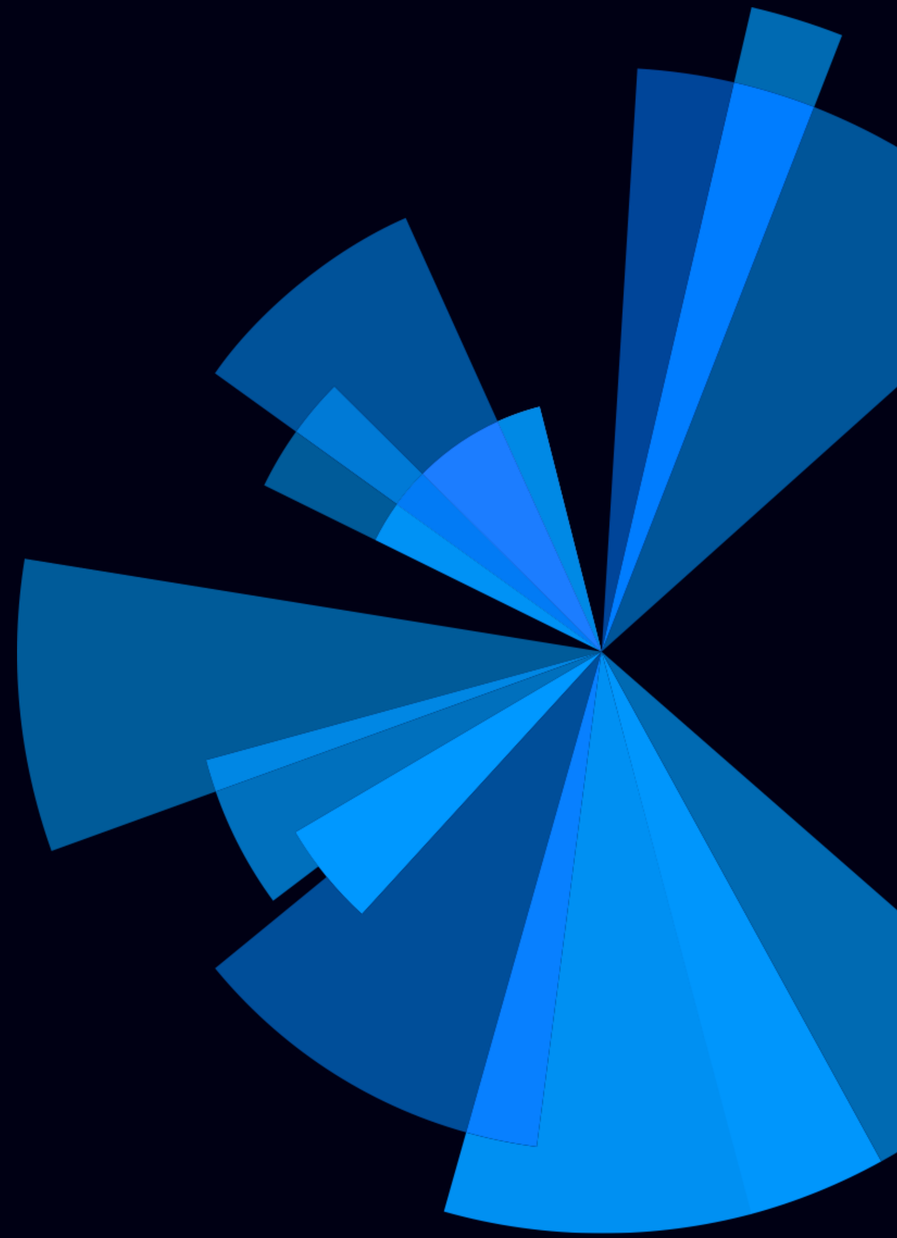
Insights

Type	Details
Full Scanning And Enumeration	Discovered Devices: 12 (5 Windows Workstations, 4 Windows Servers, 3 Other)
Host Severity Level	Critical: 10, Low: 2
Host is vulnerable to MS17-010	2 Hosts (2 Win7)
Credentials Sniffing(5.5)	7 Domain Hash Users Sniffed
AV bypass (Open sessions on host(s))	9 Hosts (3 Win7, 1 Win2008, 2 Win2016, 1 WinXP, 1 Win2019, 1 Win10)
Valuable information Gathered from End-Point (9.4)	7 Hosts (3 Win7, 1 Win2008, 1 Win2016, 1 WinXP, 1 Win2019)



Тестирование SOC

- Подготовка (20 минут):
  - Выбрать техники MITRE для проверки
  - Настроить интеграцию с SIEM
  - Определить начальную точку атаки
  - Определить масштабы теста
  - Определить уровень скрытности
  - Настроить задачу
- Тестирование (автоматически, 1 день)



Тестирование SOC - результат

Start Time	Duration	Operation Type	Categories	Techniques	Parameters	Status
Sep 09, 2020 08:44 (UTC)	00h:00m:01s	User privilege discovery using Windows Management Instrumentation	Execution, Initial Access	Windows Management Instrumentation(T1047), Valid Accounts(T1078)	Username: healthmailbox491cc1e, Domain: LAB.UPG, Protocol: WMI, Por...	no results
Sep 09, 2020 08:44 (UTC)	00h:00m:05s	Stored Credentials Extraction from Remote Connection Managers	Credential Access	Credentials in Files(T1081), Credentials in Registry(T1214)	Ipv4: 192.168.10.23, Domain: LAB.UPG, Os: 10, Arch: x64, Username:...	success
Sep 09, 2020 08:44 (UTC)	00h:00m:00s	User privilege discovery using Remote Service API	Execution, Initial Access	Service Execution(T1035), Valid Accounts(T1078)	Username: healthmailbox491cc1e, Domain: LAB.UPG, Protocol: SMB, Ipv...	no results
Sep 09, 2020 08:44 (UTC)	00h:00m:03s	Privilege Validation using Wmi over RDP	Execution, Lateral Movement	Windows Management Instrumer		
Sep 09, 2020 08:44 (UTC)	00h:00m:00s	User privilege discovery using Windows Management Instrumentation	Execution, Initial Access	Windows Management Instrumer		
Sep 09, 2020 08:44 (UTC)	00h:00m:01s	User privilege discovery using Remote Service API	Execution, Initial Access	Service Execution(T1035), Valid A		
Sep 09, 2020 08:44 (UTC)	00h:00m:08s	SAM/NTDS.DIT Credential Extraction	Credential Access	Credential Dumping(T1003)		
Sep 09, 2020 08:43 (UTC)	00h:00m:06s	Stored Credentials Extraction from Remote Connection Managers	Credential Access	Credentials in Files(T1081), Cred		
Sep 09, 2020 08:43 (UTC)	00h:00m:22s	Privilege Validation using Wmi over RDP	Execution, Lateral Movement	Windows Management Instrumer		
Sep 09, 2020 08:43 (UTC)	00h:00m:00s	User privilege discovery using Remote COM Objects	Lateral Movement, Initial Access	Distributed Component Object M		

SIEM Integration

Import Certificate File | Import Key File | Import CA File

Enable Integration

Host IP *
192.168.10.39

Port *
514

Protocol *
UDP

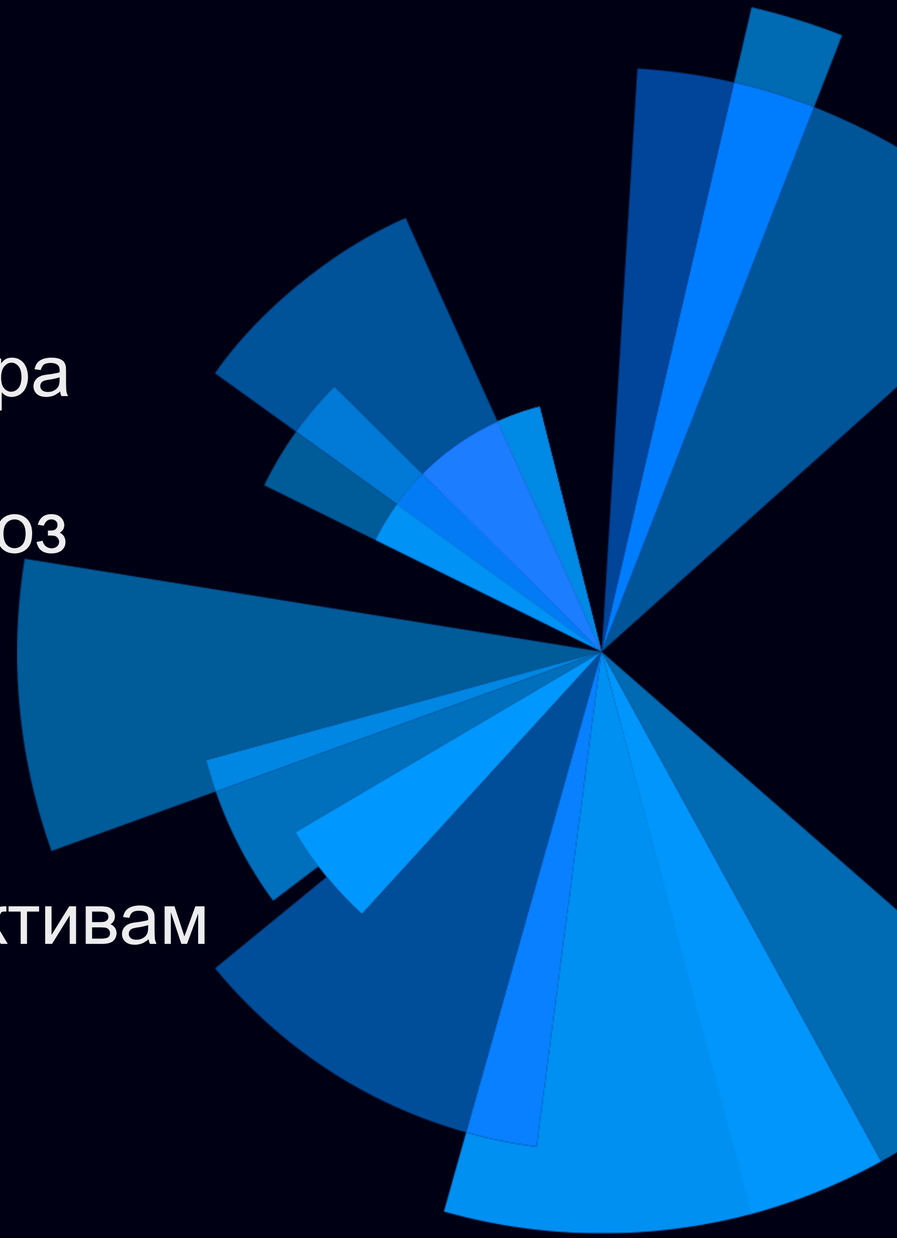
SIEM Format *
CEF (ArcSight

Let PenTera Generate Certificate

Save Configuration

Преимущества PenTera

- Не требует экспертных знаний
- Не требует постоянного участия оператора
  Быстрое получение ценных результатов
- Проверка самых актуальных техник и угроз
- Безопасная эксплуатация
- Полное представление о векторе атаки
- Высокоуровневая категорийная оценка
- Тестирование специфичных сценариев
- Демонстрация векторов атак к ценным активам
- Экономически эффективный подход



Остались вопросы?

Мы готовы на них ответить:

vfilin@citum.ru
+7(903)765-3862

Подробнее о Pcysys PenTera – на нашем сайте:
https://citum.ru/pcysys