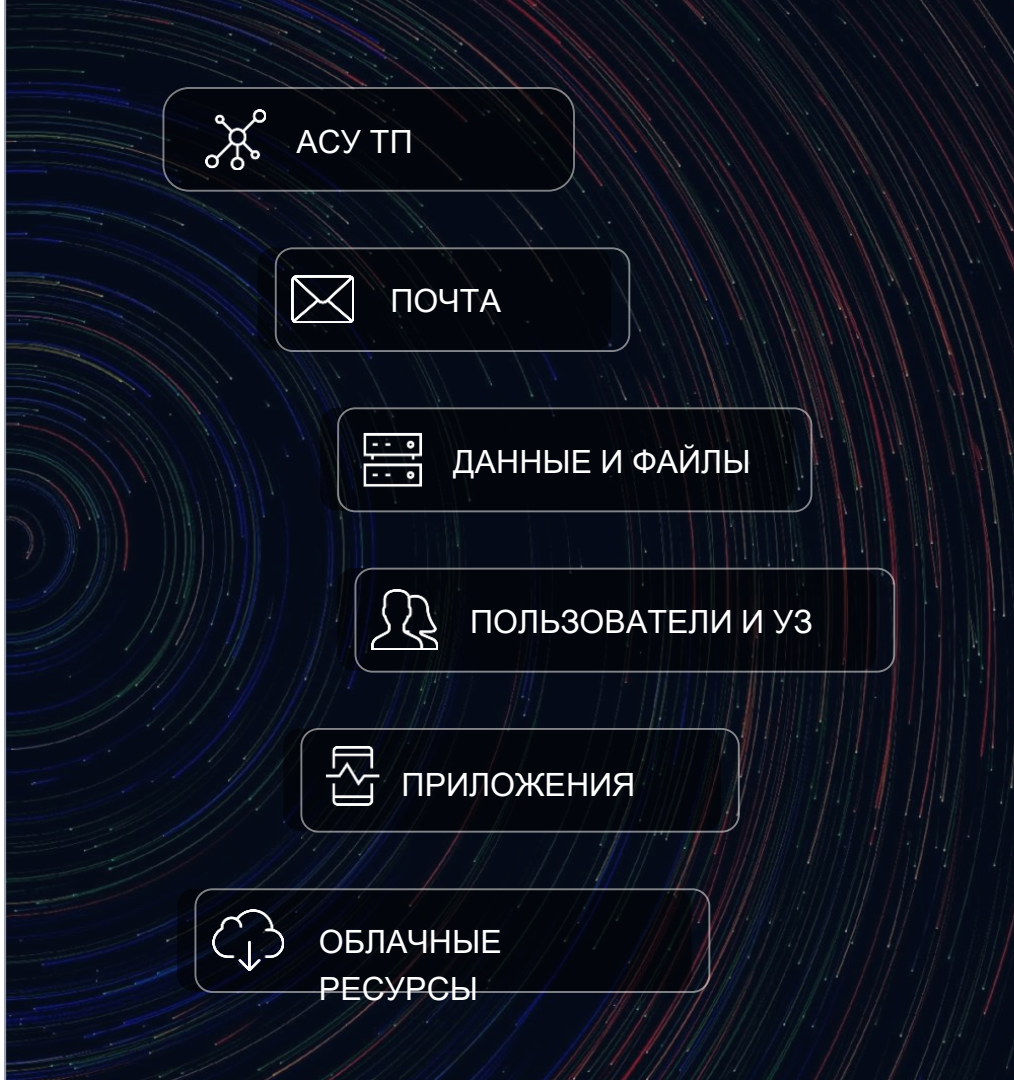
Tenable.ad
Аудит, лучшие практики и защита от атак на Active Directory

Илья Батетников, Тайгер Оптикс

Проблематика безопасности Active Directory

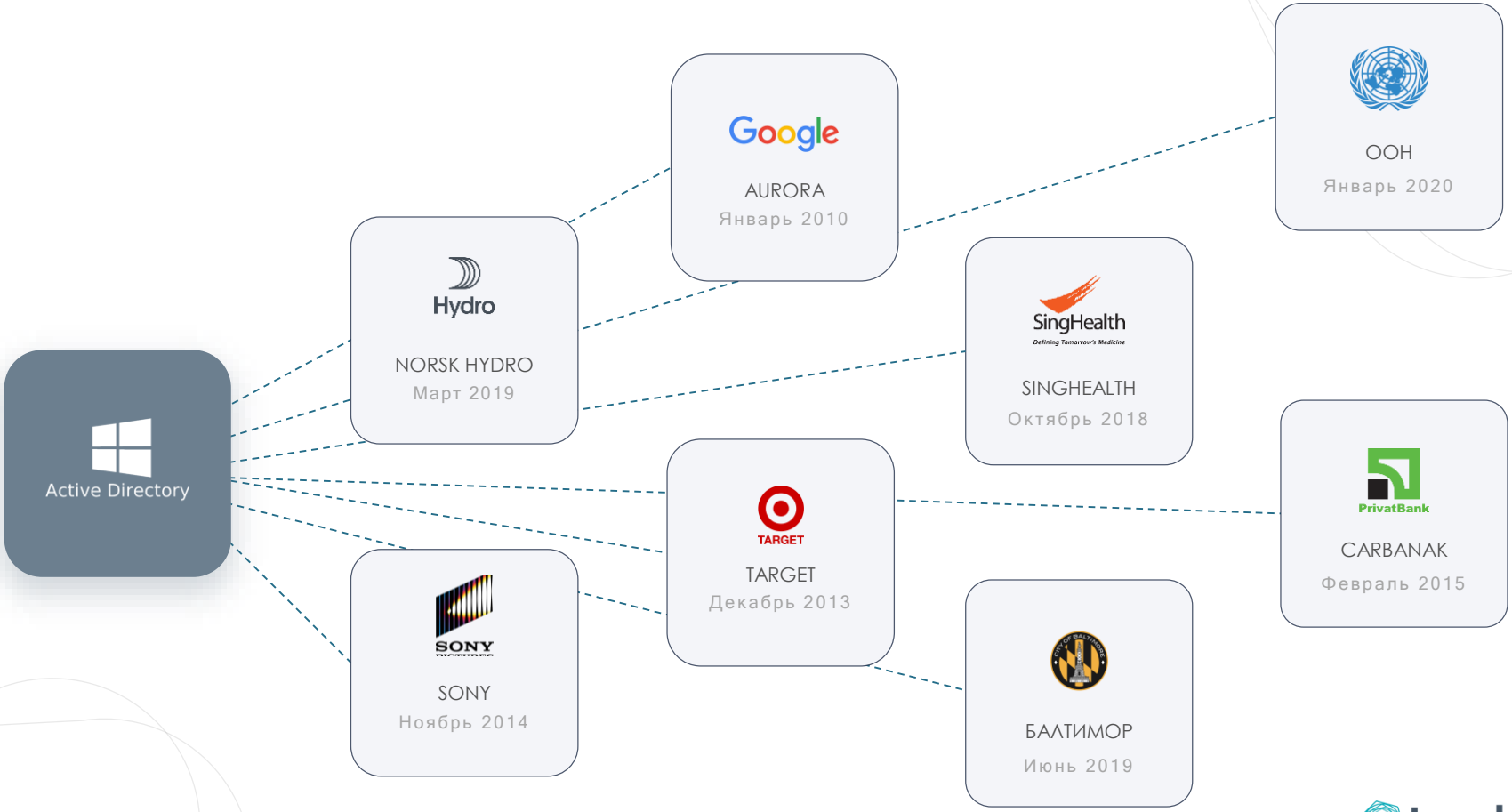
Active Directory хранит ключи от вашего царства

- Вся аутентификация, все пароли
- Права доступа ко всем активам
- Сложная, меняющаяся архитектура, которая имеет свойство выходить из-под контроля



ПОЧТИ ЗА КАЖДОЙ НОВОСТЬЮ О ВЗЛОМЕ СТОИТ НЕЗАЩИЩЕННАЯ ACTIVE DIRECTORY

tenable


Active Directory
Google
AURORA
Январь 2010
Hydro
NORSK HYDRO
Март 2019
SONY
SONY
Ноябрь 2014
TARGET
TARGET
Декабрь 2013
SingHealth
Defining Tomorrow's Medicine
SINGHEALTH
Октябрь 2018
БАЛТИМОР
Июнь 2019
ООН
Январь 2020
PrivatBank
CARBANAK
Февраль 2015
tenable

60%

НОВЫХ ВРЕДОНОСОВ СОДЕРЖАТ КОД, НАЦЕЛЕННЫЙ НА ACTIVE DIRECTORY

RYUK

ИСПОЛЬЗОВАЛ CVE-2020-1472 ДЛЯ ЭСКАЛАЦИИ ОТ ФИШИНГА ДО ДОМЕН-АДМИНА ЗА 5 ЧАСОВ

80%

ОРГАНИЗАЦИЙ, КОТОРЫМ БЫЛ ПРОВЕДЕН АУДИТ, ИМЕЛИ КРИТИЧЕСКИЕ ОШИБКИ В КОНФИГУРАЦИИ ACTIVE DIRECTORY

>95%

ОРГАНИЗАЦИЙ ИСПОЛЬЗУЮТ ACTIVE DIRECTORY

tenable

ТАЙГЕР ОПТИКС

«К примеру, по итогам пентеста в одной компании мы пришли к выводу, что:

- все доступные машины в домене были не ниже Windows10/Windows Server2016,
- на них стояли все самые свежие патчи
- сеть регулярно сканировалась, машины хардились.
- Все пользователи сидели через токены и не знали свои «20-символьные пароли».

Вроде все хорошо, но протокол IPv6 не был отключен.

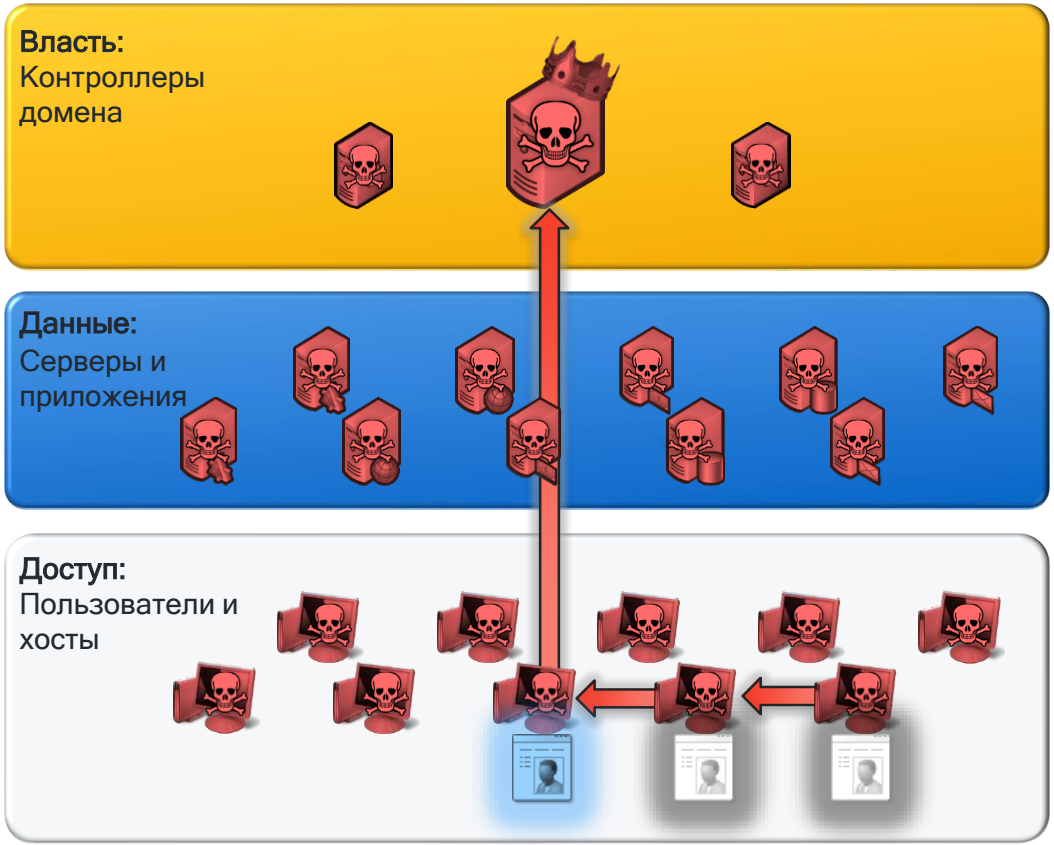
Схема захвата домена выглядела так: mitm6 -> ntlmrelay -> атака через делегирование -> получен хеш пароля локального администратора -> получен хеш пароля администратора домена.

К сожалению, такие популярные сертификации, как OSCP, GPEN или CEH, не учат проведению тестирования на проникновение Active Directory. »

https://habr.com/ru/company/jetinfosystems/blog/449278/

tenable

Типичный сценарий атаки с использованием Active Directory



1. Первоначальное проникновение на машину пользователя (фишинг, эксплойт в браузере, PDF, Java, MS Office и т.д.)
2. Рабочая станция взломана, далее злоумышленник повышает привилегии для получения хэша пароля обычного пользователя, тикета Kerberos, пароля Windows-сервиса и т.п.
3. Злоумышленник использует этот аккаунт для латерального движения
4. Злоумышленник находит привилегированный аккаунт на рабочей станции или сервере (в идеале, администратор домена)
5. **Шоу начинается!**

Злоумышленник = Человек или ВПО

tenable

Итого: проблемы безопасности AD

1. Active Directory слишком большая и сложная. Постоянные изменения. Нет понимания, что и почему происходит с доменами или лесом AD
2. Нет навыков, опыта и времени для выявления угроз и ошибок конфигурации Active Directory
3. Алерты с DC и Win-машин захламляют SIEM, приводят к ложным срабатываниям и синдрому «мальчика, который кричал о волках»
4. Важность защиты AD игнорируется или деприоритизируются ИТ / бизнесом
5. СЗИ, используемые для мониторинга AD, не объясняют, что не так и не помогают устранять проблемы
6. Вроде покупаем и покупаем новые продукты, но пентестеры все равно взламывают нас

Защита Active Directory с помощью Tenable.ad

tenable.ad™

Прерывание большинства атак за счет блокирования латерального движения

Основана признанными специалистами IR, создателями утилиты Bloodhound

Внедрения в 15 странах, защита 100+ заказчиков с 4M+ аккаунтами

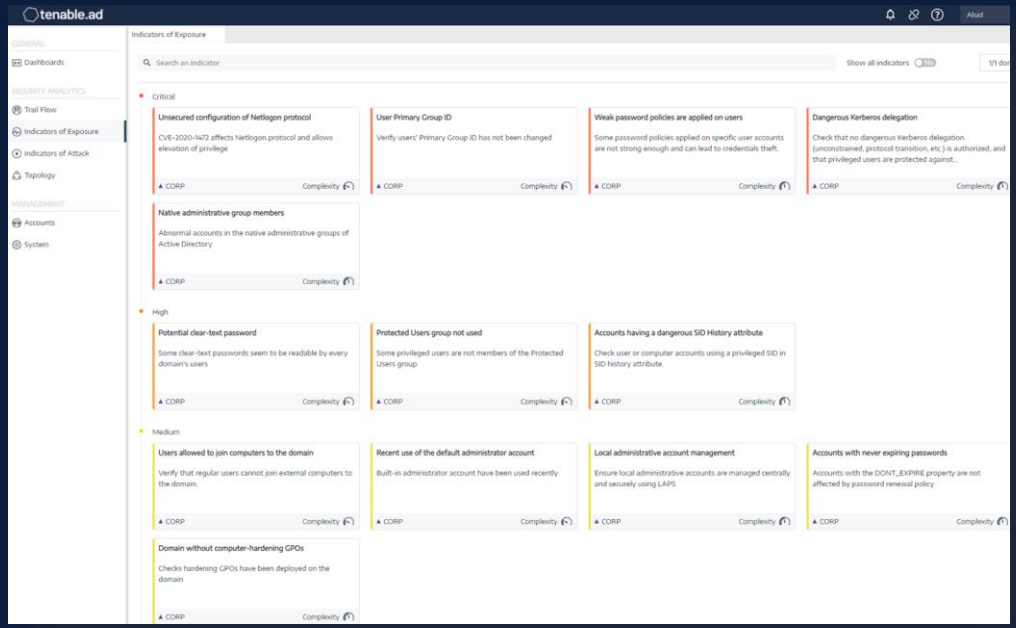
FINTECH BHP SAFRAN SANOFI sodexo UNIBAIL-RODAMCO-WESTFIELD

ЗАЩИТА ACTIVE DIRECTORY И ПРЕДОТВРАЩЕНИЕ ТРАЕКТОРИЙ АТАКИ

1. ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ СЛАБЫХ МЕСТ
2. ВЫЯВЛЕНИЕ НОВЫХ ТРАЕКТОРИЙ АТАК
3. ВЫЯВЛЕНИЕ ТЕКУЩИХ АТАК В РЕАЛЬНОМ ВРЕМЕНИ
4. РАССЛЕДОВАНИЯ И ХАНТИНГ ЗА УГРОЗАМИ

tenable.ad

- Выявление ошибок и рискованных конфигураций Active Directory
- Идентификация опасных доверительных отношений
- Детект каждого важного изменения в AD
- Выявление связей между изменениями AD и вредоносными действиями
- Выявление и детальный анализ атак на AD
- Сопоставление с индикаторами MITRE ATT&CK прямо в описании инцидентов



БЕЗ АГЕНТОВ

БЕЗ ПРИВЕЛЕГИЙ

ON-PREM ИЛИ CLOUD

РЕЗУЛЬТАТ СРАЗУ

Проблемы с конфигурацией AD, которые выявляет Tenable.ad

Эскалация привилегий	Бэкдоринг	Рискованные конфигурации безопасности
1. (C) Privileged accounts running Kerberos services 2. (C) Dangerous Kerberos delegation 3. (C) Use of weak cryptography algorithms into Active Directory PKI 4. (C) Dangerous access rights delegation on critical objects 5. (U) (M) Multiple issues in the password policy 6. (C) Dangerous RODC management accounts 7. (C) Sensitive GPO linked to critical objects 8. (U) Administrative accounts allowed to connect to other systems than the Domain Controllers 9. (C) Dangerous trust relationship 10. (C) Reversible passwords in GPO 11. (M) Computers running an obsolete OS 12. (U) (M) Accounts using a pre-Windows 2000 compatible access control 13. (U) Local administrative account management 14. (U) Dangerous anonymous users configuration 15. (C) Abnormal RODC filtered attributes 16. (U) Lacking restriction on lateral movements attack scenario 17. (M) Clear-text password stored in DC shares 18. (C) Dangerous access control rights on logon scripts 19. (C) Dangerous parameters are used in GPO 20. (U) Dangerous parameters defined in the User Account Control configuration 21. (M) Lacking application of security patches 22. (U) Brute force attempt on user accounts 23. (U) Kerberos configuration on user account 24. (M) Abnormal share or file stored on the DC	1. (C) Ensure SDProp consistency 2. (U) (M) User primary group ID 3. (C) Verify root domain object permissions 4. (C) Verify sensitive GPO objects and files permissions 5. (C) Dangerous access rights on RODC KDC account 6. (U) (M) Sensitive certificates mapped to user accounts 7. (U) Rogue Krbtgt SPN set on regular account 8. (C) KDC password last change 9. (U) (M) Accounts having a dangerous SID History attribute 10. (M) Rogue domain controllers 11. (C) Illegitimate Bitlocker key access control 12. (C) Abnormal entries in the Schema security descriptor 13. (U) DSRM account activated 14. (C) Dangerous caching policy on RODC 15. (C) Certificate deployed by GPO applied on DC 16. (U) Authentication hash not renewed when using smartcard 17. (U) Reversible passwords for User accounts 18. (C) Use of explicit denied access on containers	1. (U) (M) Native administrative group members 2. (U) Accounts with never expiring passwords 3. (U) Recent use of the default administrator account 4. (C) Protected Users group not created or not used 5. (C) Presence of blocking OU 6. (M) Inappropriate number of Domain Controllers 7. (C) Unlinked, disabled or orphan GPO 8. (U) (M) Sleeping accounts 9. (U) (M) AdminCount attribute set on standard users 10. (U) (M) Disabled accounts in privileged groups 11. (C) Domains have an outdated functional level 12. (C) Domain using a dangerous backward-compatibility configuration 13. (U) Lacking the use of Managed Service Accounts 14. (C) Lacking the use of Advanced Audit Policy 15. (C) Lack of Active Directory backups 16. (U) (M) Regular users can add new computers into AD domain 17. (C) Active Directory event logs not centralized 18. (U) (M) Account naming convention not fully respected 19. (C) Use of non-canonical ACE

Значения типов индикаторов в названиях индикаторов

- U = User, пользователь
- M = Machine, машина
- C = Security Component, компонент безопасности

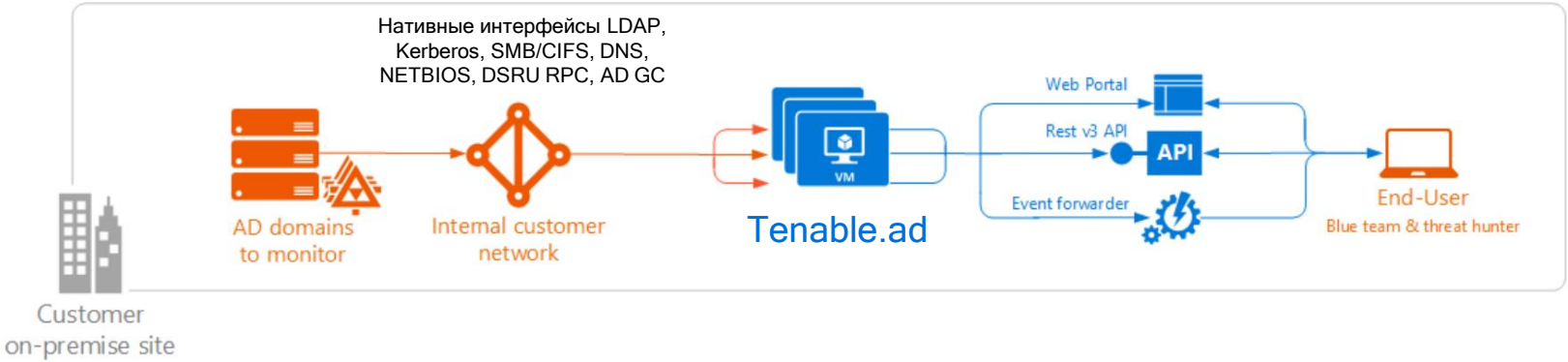
tenable

Неполный список ВПО и атак, от которых защищает Tenable.ad

1. Kerberom
2. Nishang
3. ANSSI-ADCP
4. BloodHound
5. Patator
6. Impacket
7. CrackMapExec
8. Kekeo
9. SMB Password crawler
10. Metasploit
11. Mimikatz (DCShadow)
12. SMBSpider
13. Responder
14. Mimikatz (LSADump)
15. Mimikatz (Silver Ticket)
16. Mimikatz (Golden Ticket)
17. Mimikatz (DCSync)
18. DeathStar
19. Mimikatz (Token Impersonate)
20. GPOInjection
21. Enum
22. Empire
23. Password Spraying

tenable

Архитектура Tenable.ad



SANOFI

«Развернув Tenable.ad по всей компании, мы получили важнейшую информацию о наших рисках»

350K+
АККАУНТОВ

35+
СТРАН

85+
САЙТОВ

Lagardère

«Мы не только внедрили Tenable.ad за один день, но и обеспечили эффективный мониторинг безопасности индивидуальных инфраструктур, не влияя на нагрузку специалистов по безопасности»
Lagardere, 30.000 сотрудников, 40 стран

Спасибо!
Закажите тестирование Tenable.ad

sales@tiger-optics.ru
https://www.tiger-optics.ru/get-demo/tenable-ad/