

一、EDR

1. 什么是EDR

EDR (Endpoint Detection and Response, 端点检测和响应) 是Gartner的安东·丘瓦金 (Anton Chuvakin) 创造的一个术语, 用来指代一种端点安全防护解决方案。它记录端点上的行为, 使用数据分析和基于上下文的信息检测来发现异常和恶意活动, 并记录有关恶意活动的数据, 使安全团队能够调查和响应事件。端点可以是员工终端PC或笔记本电脑、服务器、云系统、移动设备或物联网设备等。EDR解决方案通常提供威胁搜寻、检测、分析和响应功能。

(1) EDR与XDR、MDR的区别

- XDR (Extended Detection and Response, 扩展检测和响应) 是一项仍在兴起但发展迅速的技术, 是一种端点威胁检测和响应的新方法。EDR关注的是端点的数据, 而XDR中的“X”代表“扩展”, 它代表任何数据源, 不仅是端点, 还有网络、电子邮件、应用程序、云工作负载等等。
- MDR (托管检测和响应服务)。MDR可被理解为托管的XDR。

(2) EDR的功能

1. 持续收集端点数据
2. 实时分析和威胁检测
3. 自动威胁响应
4. 溯源深度处置
5. 支持威胁搜寻和安全加固

(3) openedr

官网地址 <https://www.openedr.com/>

A. 安装

1. 注册账号



* Name

The field is required

* Email

* Password

* Password (Confirm)

* Phone Number

2. Skip跳过二次验证



OPENEDR

Provided by XCITUM

2FA Account Configuration Needed

Please setup your two-factor authentication application for added account security. Your first enrolled endpoint will automatically be enabled with 2FA. Authentication is required if you enroll more than 50 managed devices. If you wish to skip, this will automatically disable two-factor authentication but can be setup at a later time.

Highly recommend to begin the 2fa setup

[Configure authentication](#)

[Skip](#)

3. 打开一台Windows 访问 Step 1 给出的下载链接（建议虚拟机，例如Windows Server 2016）


☐ Don't show next time

✓ Welcome


✓ Step 1

Step 2


Step 3


Provided by X C I T I U M

Download the OpenEDR Communication Agent with this link, and install it on each endpoint to be included in endpoint device list.

 Windows

<https://lobelapels0hicloudcom.itsm-us1.comodo.com:443/enroll/d>



▶ Learn how to enroll a device

📅 You can book an appointment here for our team to help you enroll your device

Next >

<https://lobelapels0hicloudcom.itsm-us1.comodo.com:443/enroll/device/by/token/9d7932954b46384b75200a50d4743d8d>

Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

Installer

Download Windows Installer

Installation Instruction



Step 1

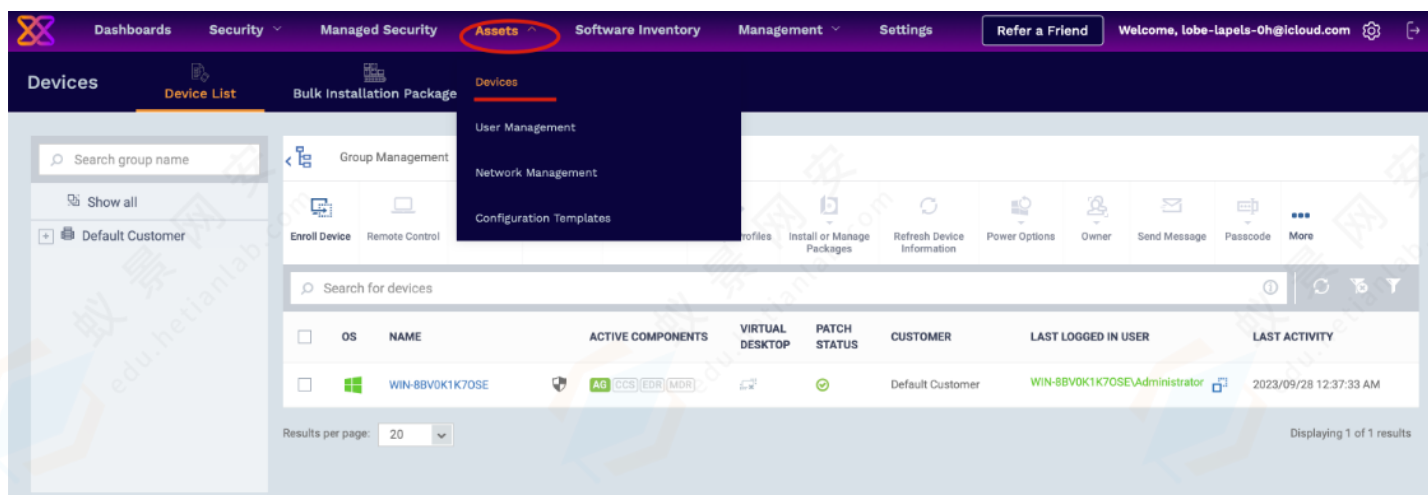
Run installer of Communication Client after download complete



Step 2

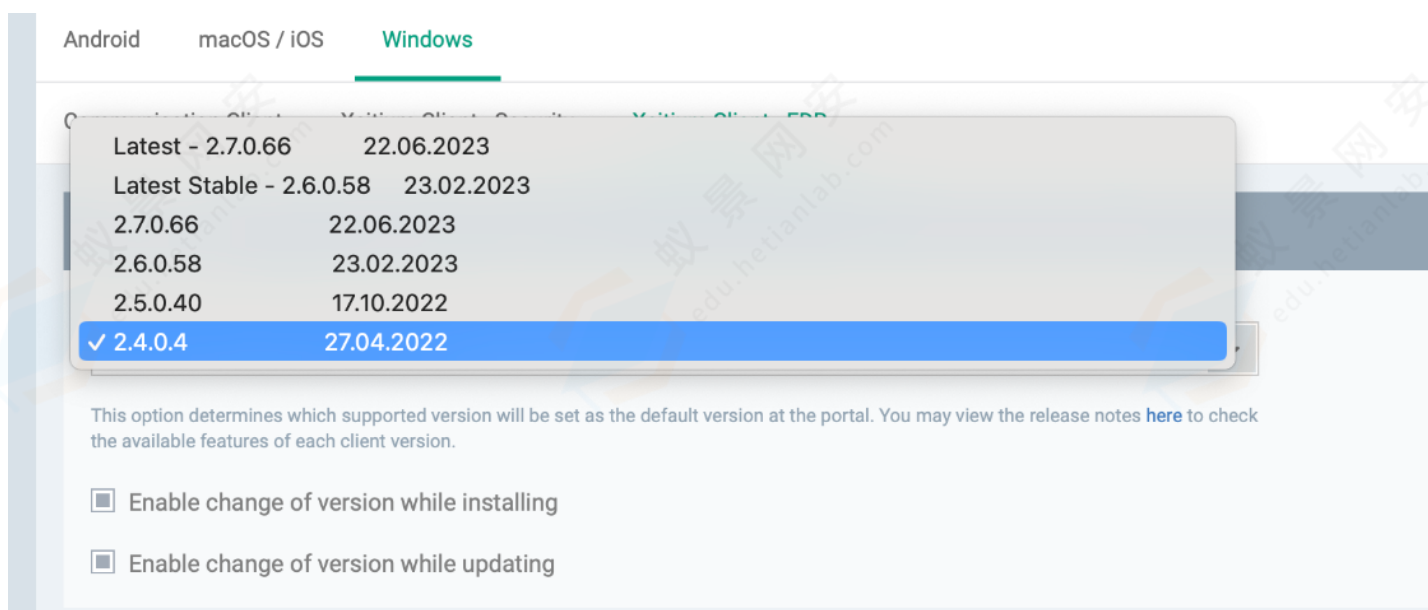
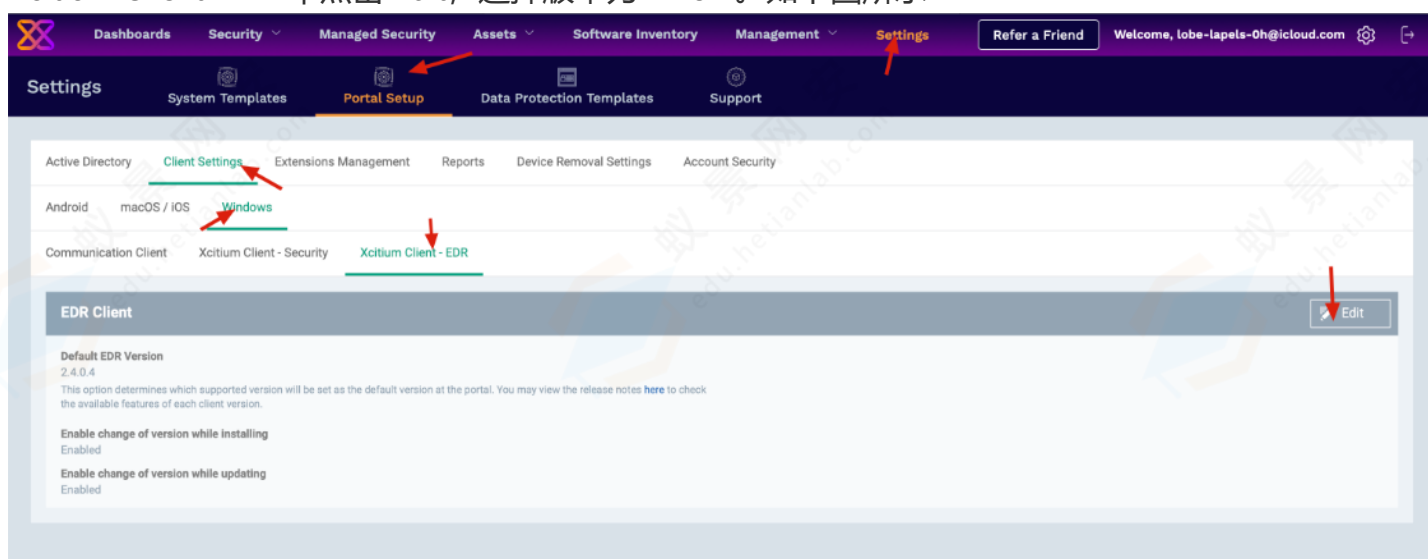
Your device will be enrolled and appears in Device List

4. 安装好后在Assets -> Devices 就能够看到自己的Windows Server 2016 （这时并没有EDR功能）

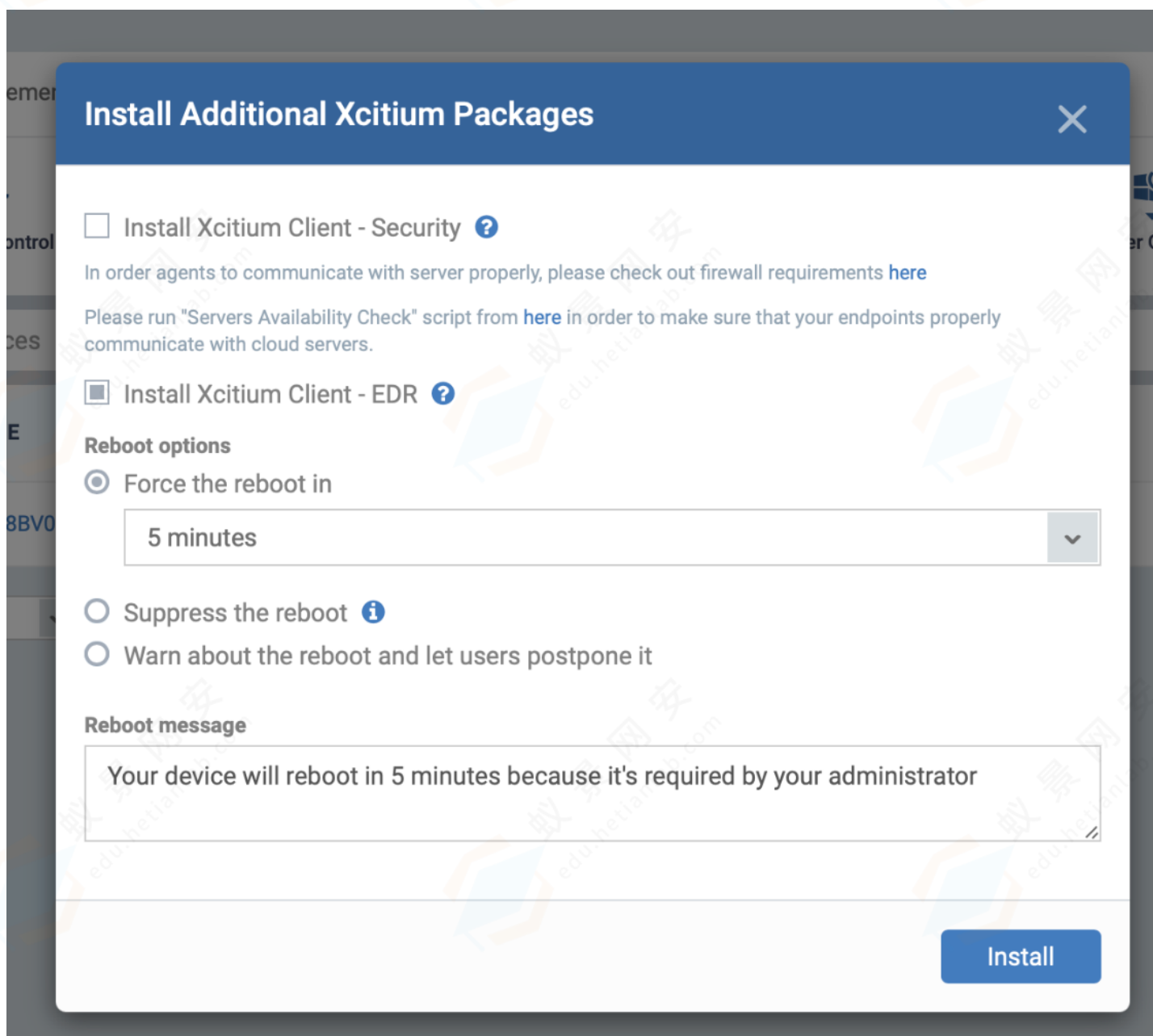
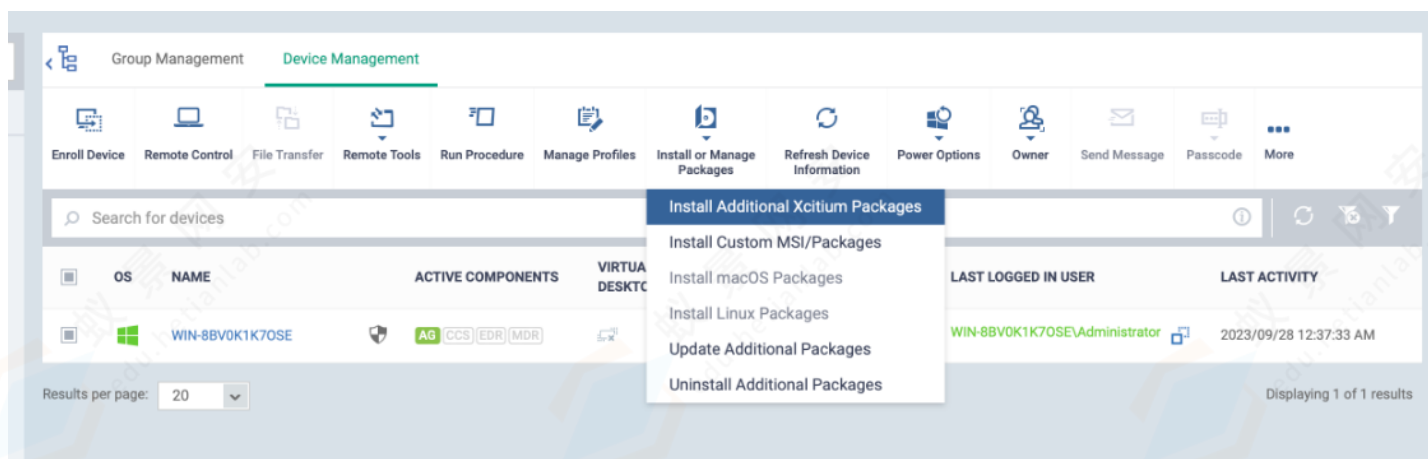


5. 为Windows server 2016 添加 EDR功能

默认的EDR客户端是不支持Windows Server 2016 的，需要到 Settings -> Client Settings -> Windows -> Xcitium Client -EDR 中点击 Edit，选择版本为2.4.04。如下图所示



调整好后就可以安装EDR了



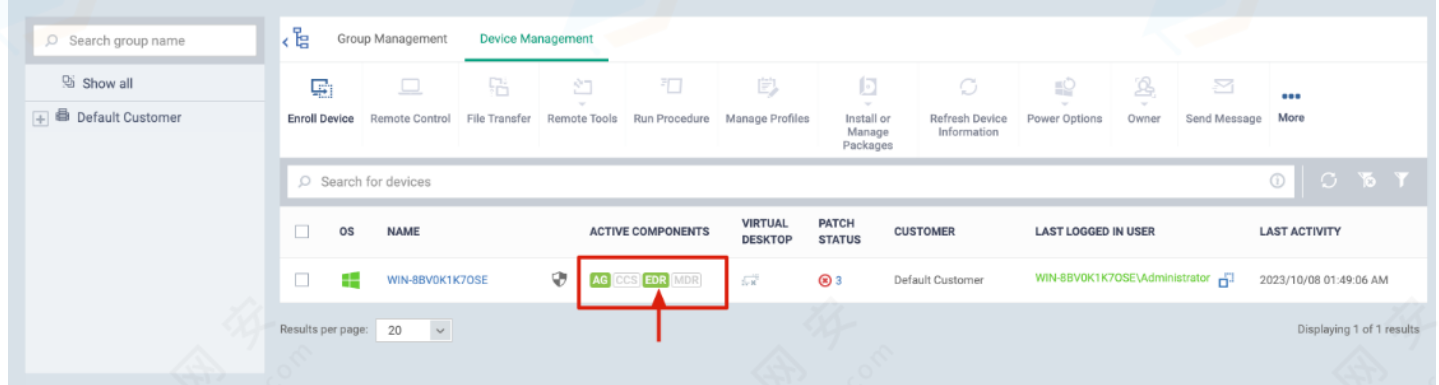
点击Install后，windows server 2016会出现如下提示（可以等五分钟自动重启，也可以点关闭然后手动重启）

即将注销你的登录

Your device will reboot in 5 minutes because it's required by your administrator

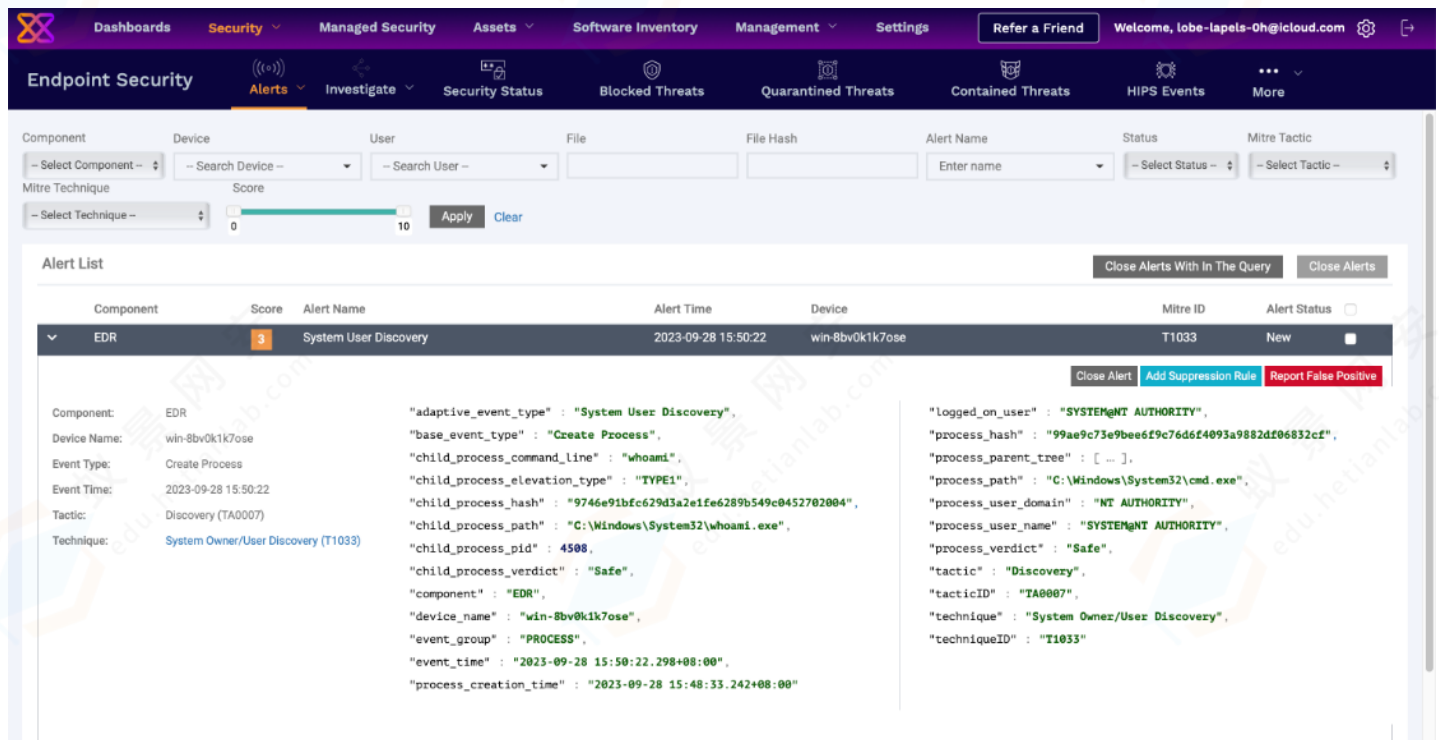
关闭(C)

重启后刷新页面，如果发现设备中的 EDR 显示绿色，就安装成功了。



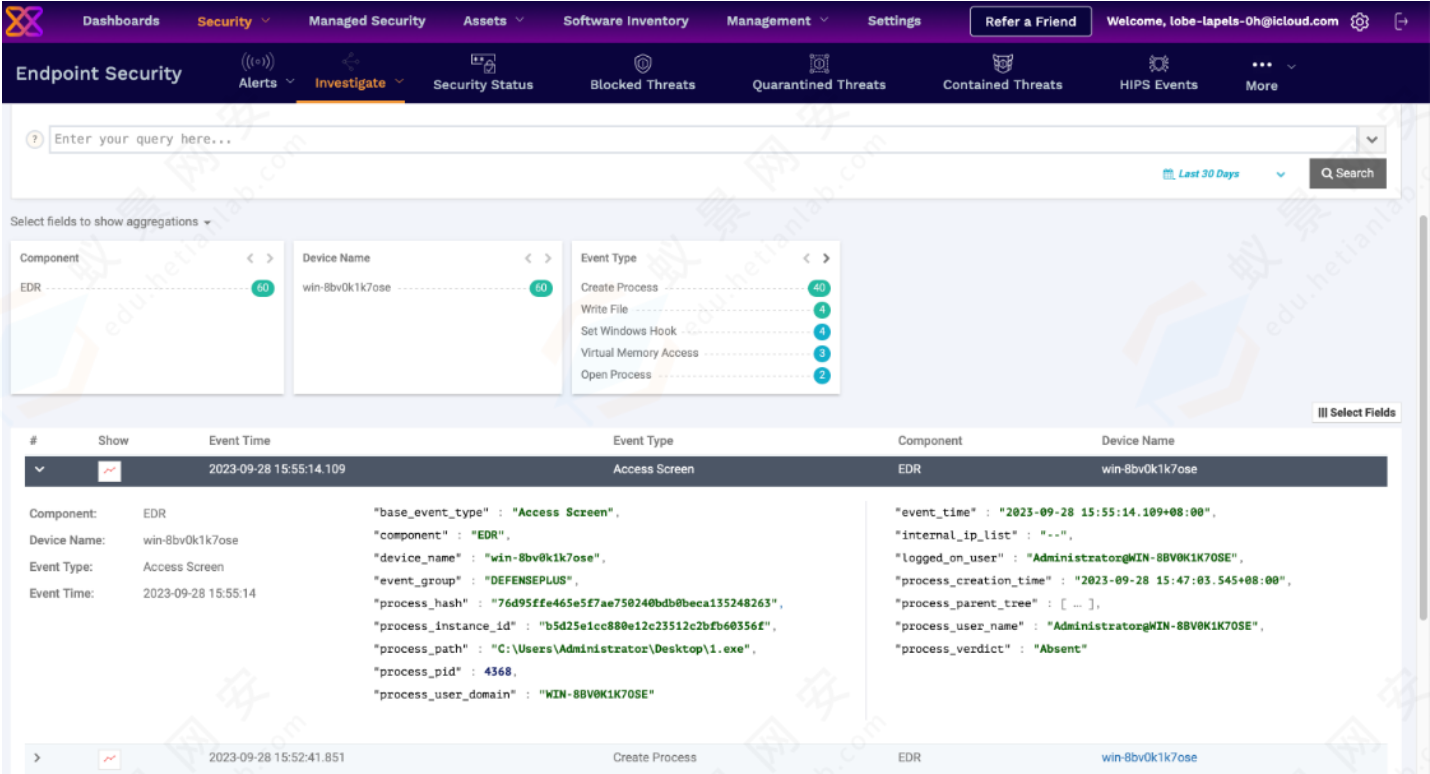
B. 使用

1. Security -> Alerts 记录安全告警

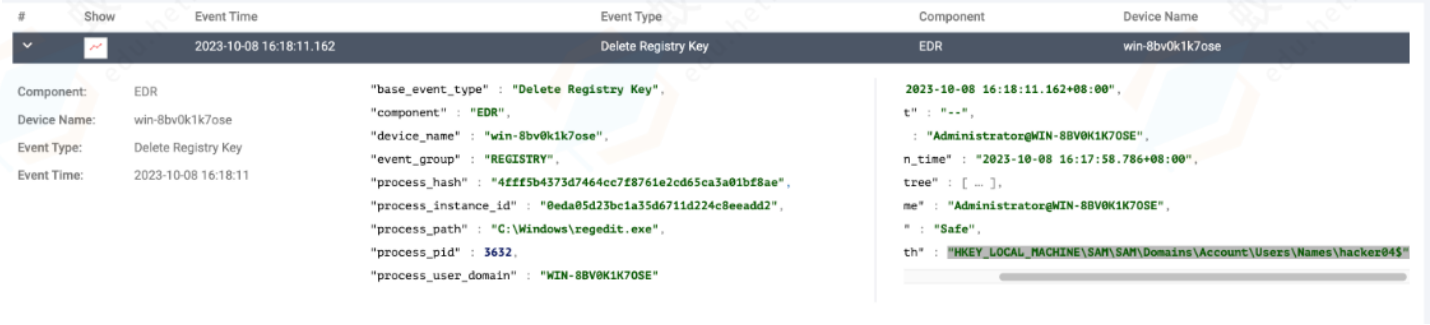


2. Security -> Investigate 记录所有活动

如下图所示，桌面的1.exe程序尝试访问屏幕（截图）



如下图，删除注册表 hacker04\$ 项



3. 设备管理



2. WAF

(1) 什么是WAF

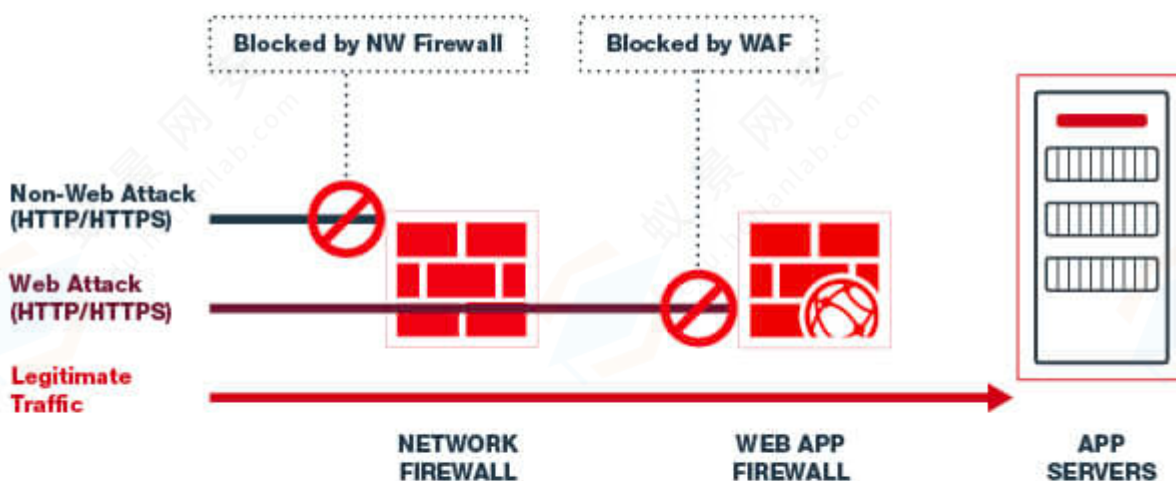
Web应用防火墙（Web Application Firewall，简称WAF）是通过执行一系列针对HTTP/HTTPS的安全策略来专门为Web应用提供保护的一款产品，主要用于防御针对网络应用层的攻击，像SQL注入、跨站脚本攻击、参数篡改、应用平台漏洞攻击、拒绝服务攻击等。

(2) WAF与网络防火墙的区别

WAF 位于外部用户和 Web 应用程序之间，以分析所有 HTTP 通信。然后，它会在恶意请求到达用户或 Web 应用程序之前对其进行检测和拦截。因此，WAF 可以保护关键业务 Web 应用程序和 Web 服务器免受零日威胁及其他应用层攻击。WAF 变得日益重要，因为随着企业推行数字化新举措，可能会使新的 Web 应用程序和应用程序编程接口 (API) 容易受到攻击。

网络防火墙可保护安全局域网 (LAN) 免受未经授权的访问，以防止攻击风险。其主要目标是将安全区域与不安全区域分隔开，并控制这两者之间的通信。如果没有网络防火墙，任何具有公共互联网协议 (IP) 地址的计算机都可以在网络外部被访问，并且可能面临攻击风险。

WEB APPLICATION FIREWALL vs NETWORK FIREWALL



(3) WAF使用

长亭雷池: <https://waf-ce.chaitin.cn/>

官方文档: <https://waf-ce.chaitin.cn/docs/>



A. 安装

```
bash -c "$(curl -fsSLk https://waf-ce.chaitin.cn/release/latest/setup.sh)"
```

B. 登录

<https://:9443>

动态口令登录

长亭雷池 WAF

1 2 3 4 5 6

登录

获取长亭雷池 WAF 最新版

重置登录密钥

TOTP方式登录：
苹果手机 iCloud 密码管理器





令牌



设置

验证码

此验证码在接下来 5 秒钟内有效。
过期后会生成新验证码。

C. 配置防御站点

编辑站点



域名

www.example.com, 多个域名用英文逗号分隔, 支持通配符 *

端口 *

18081 开启的端口



SSL



⊕ 添加一个监听端口

上游服务器 *

http://192.168.80.128:80 需要防护的站点

备注

备注

取消

提交

最后访问的网站是

https://:开启的端口, 比如我这样配置, 最后要访问的网站是 <https://192.168.80.129:18081>

D. 功能

1. 攻击事件

长亭雷池 WAF

数据统计

攻击事件

防护站点

防护配置 >

通用配置 >

系统信息

攻击事件

攻击事件 原始日志

动作 已拦截

攻击 IP 192.168.80.129

开始时间 2023-10-09 13:50:43

域名

路径

更多

动作	攻击地址	攻击类型	攻击 IP
已拦截	http://192.168.80.129:18081/sqli-labs/Less-1/?id=1' and '1'=1	SQL 注入	192.168.80.129

20 条每页, 共 1 条

2. 防护站点详情

长亭雷池 WAF

防护站点 / 站点详情

讨论区

数据统计

攻击事件

防护站点

防护配置

通用配置

系统信息

Version 3.6.4

雷池社区版官网

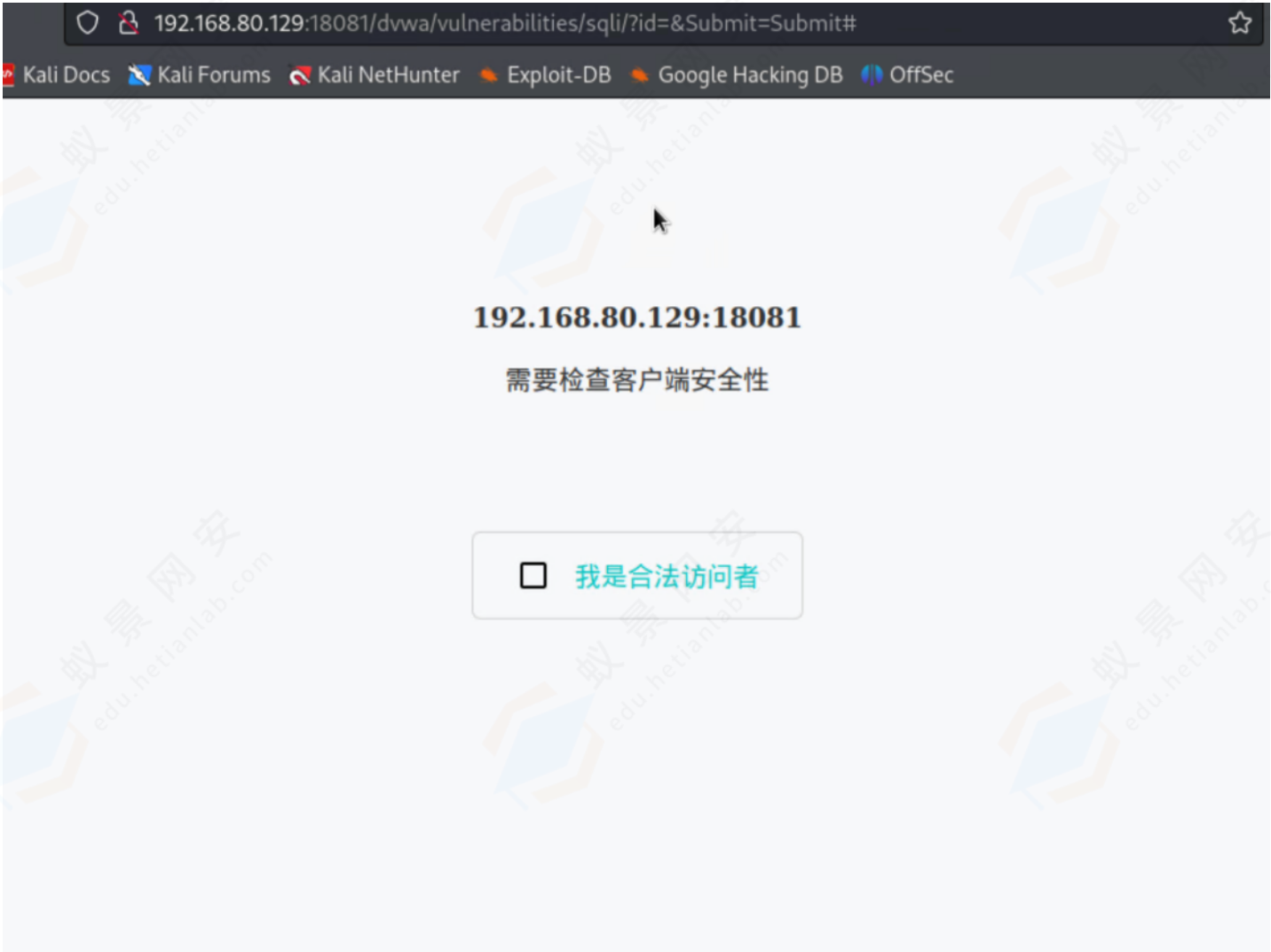
咨询企业版

通配所有域名

资源总数 23 今日请求总量 0

路径	资源类型	今日请求 / 近 30 日请求
GET /	text/html	2 / 2
/dvwa		
/dvwa		
/css		
GET /login.css	text/css	1 / 1
GET /main.css	text/css	1 / 1
GET /source.css	text/css	1 / 1
/images		
GET /lock.png	image/png	1 / 1
GET /login_logo.png	image/png	1 / 1
GET /logo.png	image/png	1 / 1

3. 防护配置



数据统计

攻击事件

防护站点

防护配置

黑白名单

频率限制

人机验证

语义分析

Version 3.6.4

雷池社区版官网

咨询企业版

高频访问限制



经过时间*

10

秒

请求次数达到*

100

次

限制结果

人机验证

限制时长*

10

分钟

保存

高频攻击限制



经过时间*

60

秒

拦截次数达到*

10

次

限制结果

直接封禁

限制时长*

30

分钟

保存

频率限制日志

搜索限制 IP

限制 IP	原因	限制结果	剩余限制时间	已限制请求数	限制开始时间
-------	----	------	--------	--------	--------