

JUNE 5, 2018

BOLEANGUARD 工控安全审计平台 用户手册

杭州木链物联网科技有限公司

浙江省杭州市西湖区西溪路 525 号浙江大学国家大学科技园 A 东 521-523

关于木链科技

杭州木链物联网科技有限公司成立于 2017 年 2 月，注册资本 558.66 万元。总部和研发中心设立在杭州西子湖畔。

公司最早由连续创业者、海归和多名来自浙江大学的优秀黑客们共同成立，后又有浙江大学 CCNT 实验室的硕士、博士研究生团队加入。

公司主营业务以工业控制网络安全审计为核心，包含工控网络监测防护产品研发销售、工业物联网大数据平台运营服务、工业物联网安全生命周期解决方案、工业物联网咨询评估、工业信息系统安全集成与定制化培训服务等。

版权声明

杭州木链物联网科技有限公司版权所有，并保留对本文档及本声明的最终解释权和修改权。本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，其著作权或其他相关权利均属于杭州木链物联网科技有限公司。未经杭州木链物联网科技有限公司书面同意，任何人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分用于商业用途。

免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

杭州木链物联网科技有限公司在编写本文档时已尽最大努力保证该文档内容准确、可靠，但杭州木链物联网科技有限公司不对本文档中的遗漏、不准确或错误导致的损失和损害承担责任。

信息反馈

如有任何宝贵意见，请反馈至：

浙江省 杭州市 西湖区 西溪路 525 号

浙江大学国家大学科技园 A 楼东区 521-523

杭州木链物联网科技有限公司

邮编 310000

或致电：0571-87216687

文档历史

时间	版本	说明	创建人
2017.7.24	1.0.0	白皮书创建	雷濛 朱奕辉
2018.1.25	1.1.1	白皮书更新	雷濛

目录

1. 产品概述	1
2. 设备安装及调试	2
2.1. 接口及指示灯介绍	2
2.2. 连接	3
2.3. 设置	3
2.4. 客户端安装	3
3. 用户登录及退出	3
3.1. 打开客户端	3
3.2. 登录审计平台	4
3.3. 登出审计平台	5
4. 用户管理	5
4.1. 账号设置	6
4.2. 用户管理	7
4.2.1. 用户列表	7
4.2.2. 新增用户	8
4.2.3. 用户编辑	9
5. 审计平台首页	12
6. 事件日志	13
6.1. 安全告警	13

6.2. 系统告警	15
6.3. 系统日志	15
7.规则管理	17
7.1. 黑名单	17
7.2. 白名单	18
7.3. IP/Mac 绑定	19
8. 资产管理	21
9.安全审计	22
9.1. 协议审计	22
9.2. 流量审计	23
10. 系统设置	23
10.1. 基础设置	23
10.2. 高级设置	24
10.2.1. 系统重置	24
10.2.2. 登录安全	24
10.2.3. 远程登录	25
11. 设备维护及常见问题处理	26
11.1. 故障诊断	26
11.2. 故障处理	26

1. 产品概述

木链工控安全审计平台是木链科技拥有自主知识产权的安全产品, 通过对控制网数据的采集、解析、鉴别, 实时动态监测通信内容, 发现并捕获异常指令和数据, 实时告警响应, 全面记录控制网中各种会话和事件, 实现对控制网信息的风险评估和对安全事件的准确回溯定位, 为工控网络安全策略的制定提供可靠的支持。

与此同时, 木链工控安全审计平台通过结合微观层面的数据语义与宏观层面的大数据分析, 实现完整的态势感知, 预判威胁与异常, 结合木链工控安全服务进一步落地安全能力。

木链工控安全审计平台的整体体系架构主要由审计中心、监控终端和选配的本地私有云构成。该体系架构如下图所示。

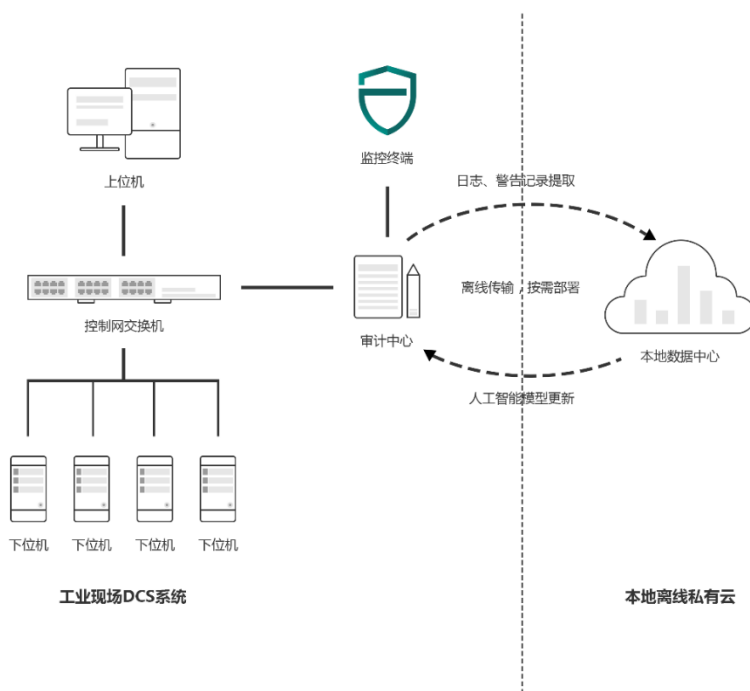


图 1-1 审计平台部署示意图

2. 设备安装及调试

2.1. 接口及指示灯介绍

端口	数量	说明
业务端口	2 个	RJ45, 10/100/1000Mbps,受限和非受限
MGMT 端口	2 个	配置、监控、管理, 连接监测审计平台和专网
USB 2.0 端口	2 个	用于系统升级, 设备配置的导出、导入, 便于维护

指示灯	状态	含义
RUN	绿灯闪烁	系统启动正常
	不亮	系统启动异常
PWR1 PWR2	绿灯长亮	电源接通
	不亮	电源无供电
HDD	闪烁	硬盘读写正常
	不亮	硬盘读写异常
LAN	Link 灯亮	LINK 正常
	Link 灯不亮	没有 LINK
	ACT 灯闪烁	有数据流量
	ACT 灯不亮	无数据流量

	全不亮	无连通链路
--	-----	-------

2.2. 连接

将审计平台的 MGMT 管理口与计算机网口通过网线直连，或者接入同一个局域网的交换机。

2.3. 设置

审计平台出厂默认的 IP 地址：192.168.86.1，子网掩码：255.255.255.0。

将管理计算机的 IP 地址设为与工业防火墙在同一网段，例如：192.168.11.xxx；子网掩码：255.255.255.0；网关（路由器）设置为防火墙的管理 IP 地址：192.168.11.11。

2.4. 客户端安装

审计平台出厂时在包装中附带客户端安装光盘，在电脑上按说明安装即可。

3. 用户登录及退出

3.1. 打开客户端

用户在桌面双击图标，打开审计平台客户端，界面如图所示。

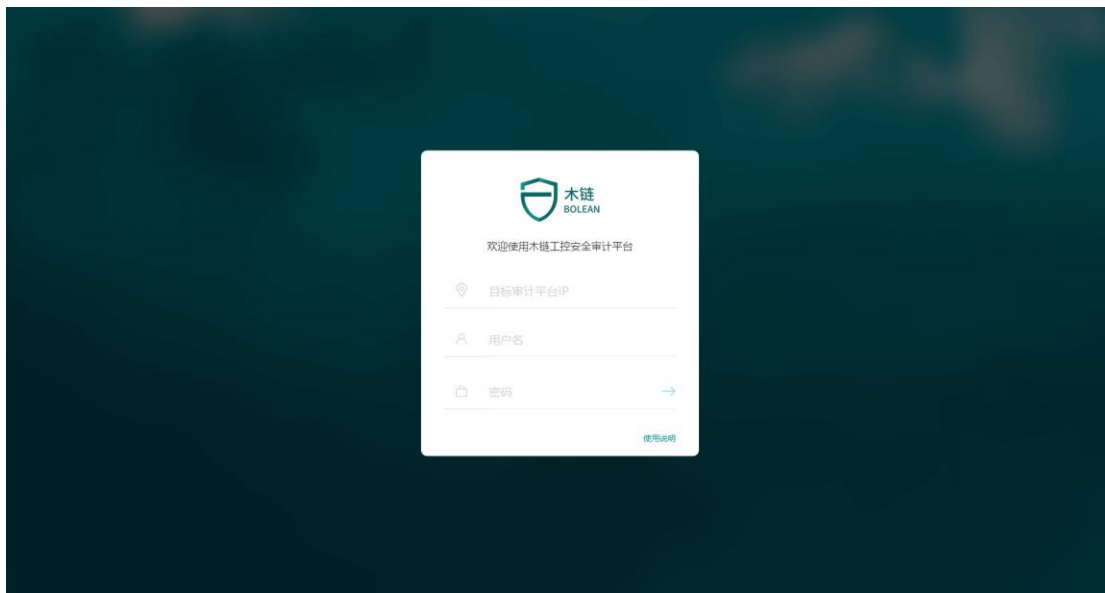


图 3-1 审计平台客户端

3.2. 登录审计平台

用户登录审计平台时需要正确填写以下信息，方可登录审计平台。

- 目标审计平台 IP

填写要访问的目标审计平台 IP 地址。设备出厂时已预置了 IP 地址。登录其他平台，，需要手动输入对应审计平台的 IP 地址。更改审计平台 IP 后，默认目标审计平台 IP 地址也将随之修改。如图所示。



图 3-2 选择目标审计平台 IP

- 账号

输入用户账号以鉴别用户身份。设备出厂时已预置了系统管理员账号。首次使用时，需以系统管理员身份登录，创建用户账号并登录后，方可使用审计平台。

- 密码

输入用户账号对应的密码，确保是账号所有者登录。

3.3. 登出审计平台

在顶部操作栏中点击“退出”按钮，即可安全登出审计平台。如图所示。

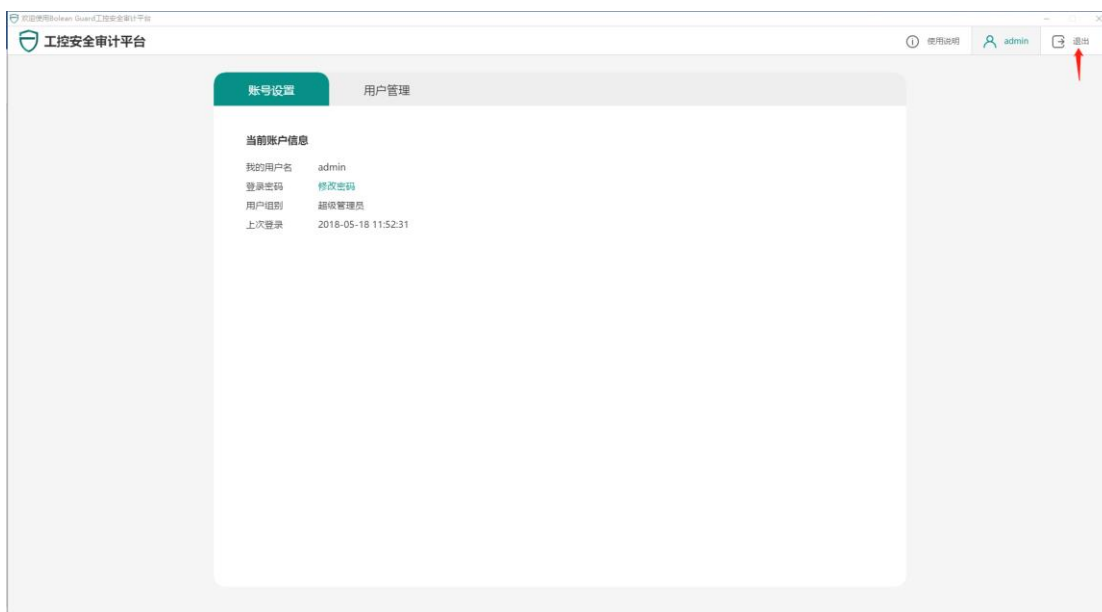


图 3-3 登出审计平台

4. 用户管理

用户在顶部操作栏中点击“用户”按钮，进入管理页面。按照用户权限不同，用户管理分为“账号设置”、“用户管理”两个功能标签。如图所示，为系统管理员的用户管理界面。

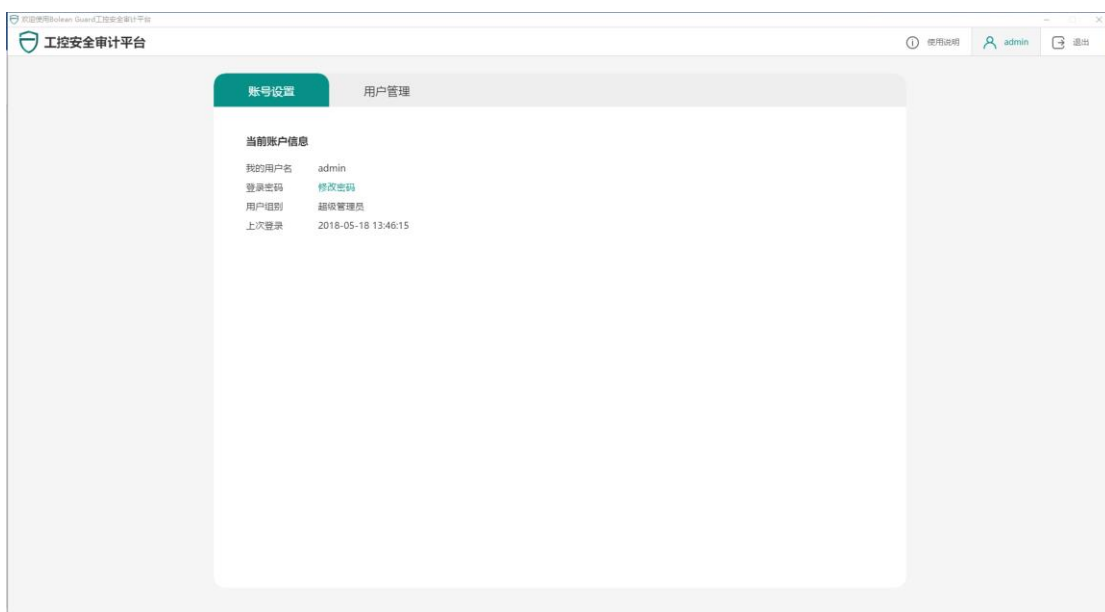


图 4-1 用户管理界面

4.1. 账号设置

账号设置功能面向所有用户角色开放。可以查看当前账户的基本信息，修改当前账户的登录密码。

用户点击“修改密码”按钮，弹出如图所示的对话框。用户按照提示正确填写信息，即可修改密码。



A modal window titled "修改密码" (Change Password) with a close button (X) in the top right corner. It contains three input fields: "原密码" (Original Password) with placeholder text "请输入当前使用的密码", "新密码" (New Password) with placeholder text "请输入新密码", and "确认密码" (Confirm Password) with placeholder text "请再次输入新密码". At the bottom is a green "确定" (Confirm) button.

图 4-2 账号设置界面

4.2. 用户管理

用户管理功能仅向系统管理员开放，可新增、查询、编辑审计平台内的各类用户账号。

4.2.1. 用户列表

点击“用户管理”标签进入用户列表，页面如图所示。

账号设置		用户管理			
当前账户信息					新增用户
用户状态	用户名	用户类型	创建时间	备注	操作
启用	admin	超级管理员	2018-04-26	系统内置的管理员，不可删除	编辑
启用	e2egcs	工程师	2018-05-17		编辑
启用	test	工程师	2018-05-16		编辑
启用	tests	工程师	2018-05-16		编辑
启用	engineer	工程师	2018-05-15		编辑
启用	eng	工程师	2018-04-27	工程师	编辑
启用	test20	工程师	2018-04-26		编辑
启用	test16	工程师	2018-04-26	123	编辑
禁用	test1	工程师	2018-04-26	123456	编辑
禁用	jinyong	操作员	2018-05-18		编辑

< 1 2 >

跳至 1 页

图 4-3 用户列表

4.2.2. 新增用户

点击“新增用户”按钮，进入如图所示的新增用户表单填写页面。按提示正确填写表单，点击“完成”按钮，即可完成新用户的增加。

当前位置：用户管理 > 新增用户

新增用户

用户名

密码

确认新密码

选择用户所在的组别 ☒ 工程师 ☐ 操作员

图 4-4 新增用户表单

用户组别的权限如下表所示。

表 4-1 用户权限表

权限	工程师	操作员
事件日志	可编辑	仅查看
规则管理	可编辑	仅查看
资产管理	可编辑	仅查看
安全审计	仅查看	仅查看
系统设置	可编辑	只可编辑基础设置
用户管理	可编辑	无权限

4.2.3. 用户编辑

在用户列表页点击“编辑”按钮，进入用户详情页。可对用户账号进行以下操作。

当前账户信息

用户名	engineer
密码	重置密码
用户状态	<input checked="" type="radio"/> 正常 <input type="radio"/> 禁用
禁用时长	无
用户组别	<input checked="" type="radio"/> 工程师 <input type="radio"/> 操作员
备注	<input type="text" value="请输入备注"/>

保存修改

> [删除账号](#)

图 4-5

- 重置密码

当用户账号的登录密码丢失时，系统管理员可帮助其重置密码。

点击“重置密码”按钮，弹出如图所示对话框，按照提示正确填写表单，即可重置密码。需要注意的是，身份验证时填写的是系统管理员账号的密码。



The dialog box is titled "重置密码" (Reset Password) and contains three input fields. The first field is labeled "新密码" (New Password) with a placeholder "请输入新密码". The second field is labeled "确认密码" (Confirm Password) with a placeholder "请再次输入新密码". The third field is labeled "进行身份验证即可重置用户密码" (Perform identity verification to reset user password) with a placeholder "请输入当前账号的密码". A green "确定" (Confirm) button is at the bottom.

图 4-6 重置密码

- 修改用户状态

用于改变用户账号的状态。由于某些原因，需要停用用户账号，或是启用某些禁用中的账号。修改用户状态后，点击“保存修改”按钮，修改生效。

- 修改用户组

用于改变用户所在的组别，即改变用户的操作权限。

- 添加备注

对用户添加备注，方便管理。

- 删除账号

用于删除已经停止使用的用户账号。点击“删除账号”按钮，弹出如图所示对话框，按照提示正确填写表单，即可删除用户账号。需要注意的是，身份验证时填写的是系统管理员账号的密码。

系统管理员账号不能删除。



图 4-7 删除用户

5. 审计平台首页

用户登录后进入首页。可查看一段时间内的审计报告、设备的运行情况、未读通知。

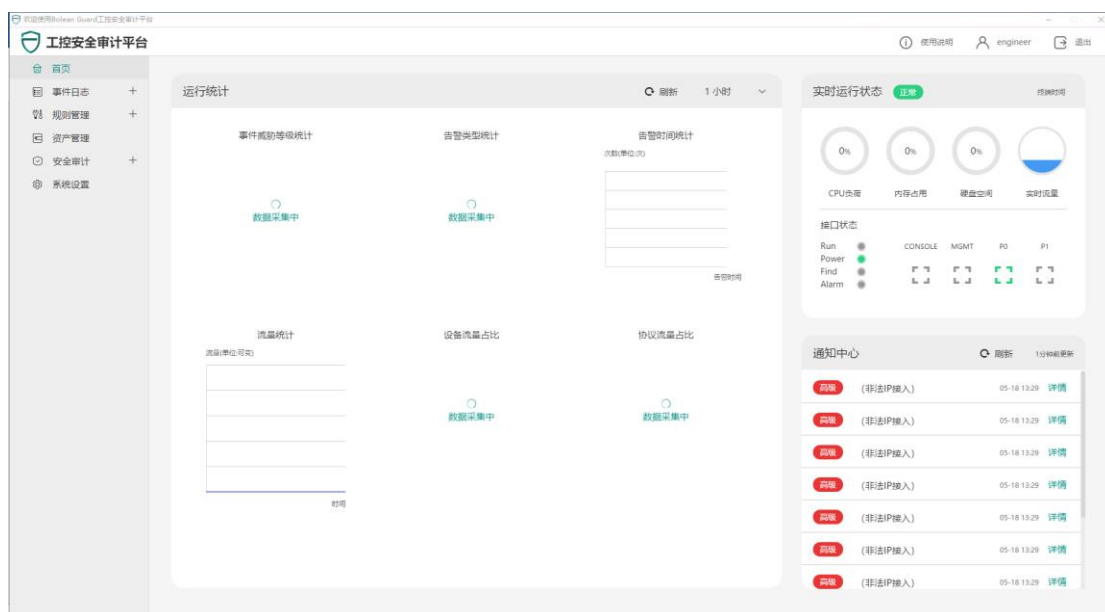


图 5-1 审计平台首页

- 运行统计

用户可切换统计时长, 查看从现在起 1 小时、24 小时、72 小时内的事件统计数据。

统计数据按不同维度分成 6 张图标。

- 实时运行状态

显示审计平台设备实时运行情况。存在异常时, 进行响应的告警。

- 通知中心

摘要显示来自安全告警、系统告警列表中最新的事件。用户可在此查看最新安全事件。

6. 事件日志

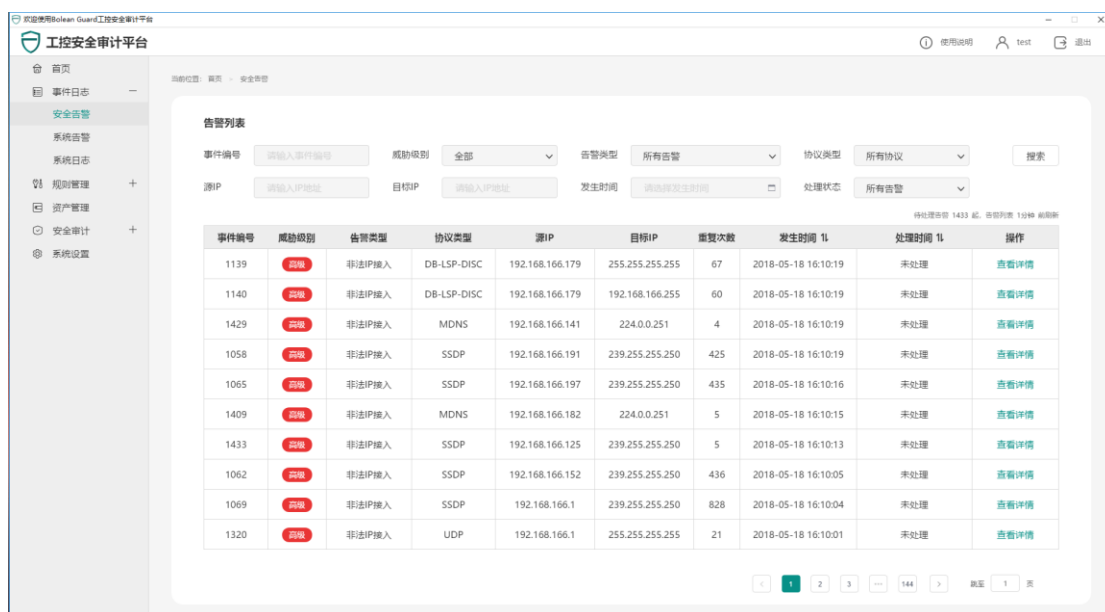
事件日志展示的是设备自运行以来的对工控网络中的流量解析、设备状态异常和规则变化等内容, 分为安全告警、系统告警与系统事件三种。

6.1. 安全告警

安全告警是指审计平台审计到的工控系统中所发生的异常事件, 如黑名单、非法 IP 接入、非法端口、Mac 地址冲突等。

安全告警事件按发生时间排列, 用户可以通过设定筛选条件或搜索关键字查看特定的事件。点击“查看详情”按钮, 进入事件详情页, 事件状态变为“已处理”, 并记录处理时间。

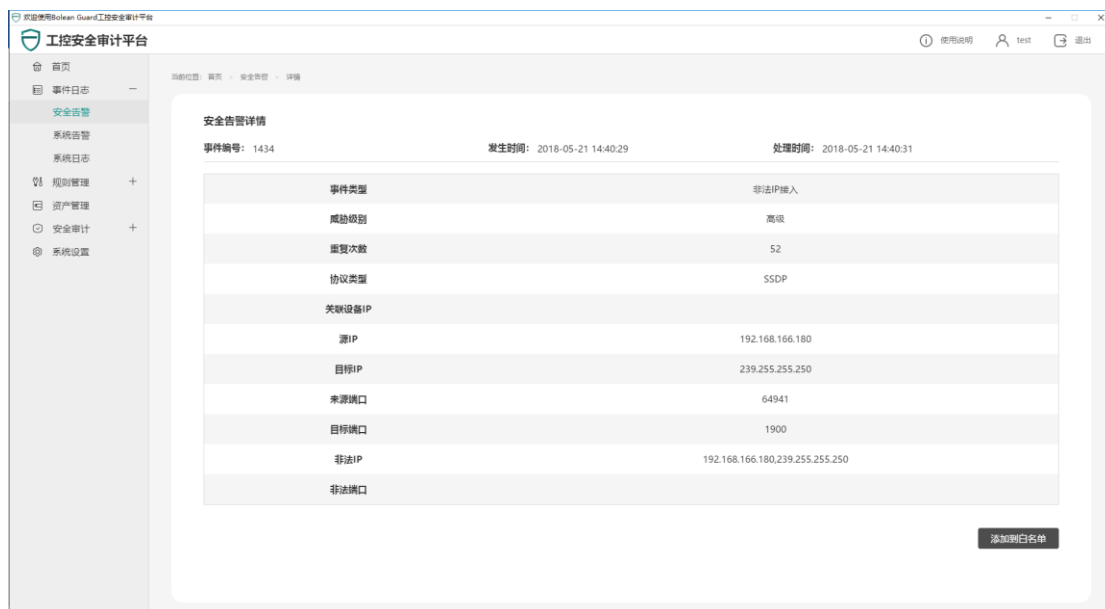
如图所示为安全告警事件列表。



事件编号	威胁级别	告警类型	协议类型	源IP	目标IP	重复次数	发生时间	处理时间	操作
1139	高危	非法IP接入	DB-LSP-DISC	192.168.166.179	255.255.255.255	67	2018-05-18 16:10:19	未处理	查看详情
1140	高危	非法IP接入	DB-LSP-DISC	192.168.166.179	192.168.166.255	60	2018-05-18 16:10:19	未处理	查看详情
1429	高危	非法IP接入	MDNS	192.168.166.141	224.0.0.251	4	2018-05-18 16:10:19	未处理	查看详情
1058	高危	非法IP接入	SSDP	192.168.166.191	239.255.255.250	425	2018-05-18 16:10:19	未处理	查看详情
1065	高危	非法IP接入	SSDP	192.168.166.197	239.255.255.250	435	2018-05-18 16:10:16	未处理	查看详情
1409	高危	非法IP接入	MDNS	192.168.166.182	224.0.0.251	5	2018-05-18 16:10:15	未处理	查看详情
1433	高危	非法IP接入	SSDP	192.168.166.125	239.255.255.250	5	2018-05-18 16:10:13	未处理	查看详情
1062	高危	非法IP接入	SSDP	192.168.166.152	239.255.255.250	436	2018-05-18 16:10:05	未处理	查看详情
1069	高危	非法IP接入	SSDP	192.168.166.1	239.255.255.250	828	2018-05-18 16:10:04	未处理	查看详情
1320	高危	非法IP接入	UDP	192.168.166.1	255.255.255.255	21	2018-05-18 16:10:01	未处理	查看详情

图 6-1 安全告警列表

如图所示为查看告警事件的详情。针对非法 IP，核实无害后可将其快速添加到白名单列表中。



安全告警详情	
事件编号: 1434	发生时间: 2018-05-21 14:40:29
处理时间: 2018-05-21 14:40:31	
事件类型	非法IP接入
威胁级别	高危
重复次数	52
协议类型	SSDP
关联设备IP	
源IP	192.168.166.180
目标IP	239.255.255.250
来源端口	64941
目标端口	1900
非法IP	192.168.166.180, 239.255.255.250
非法端口	

图 6-2 安全告警详情

6.2. 系统告警

系统告警是指审计平台设备自身异常时进行告警提示，主要为 CPU 告警和存储告警。

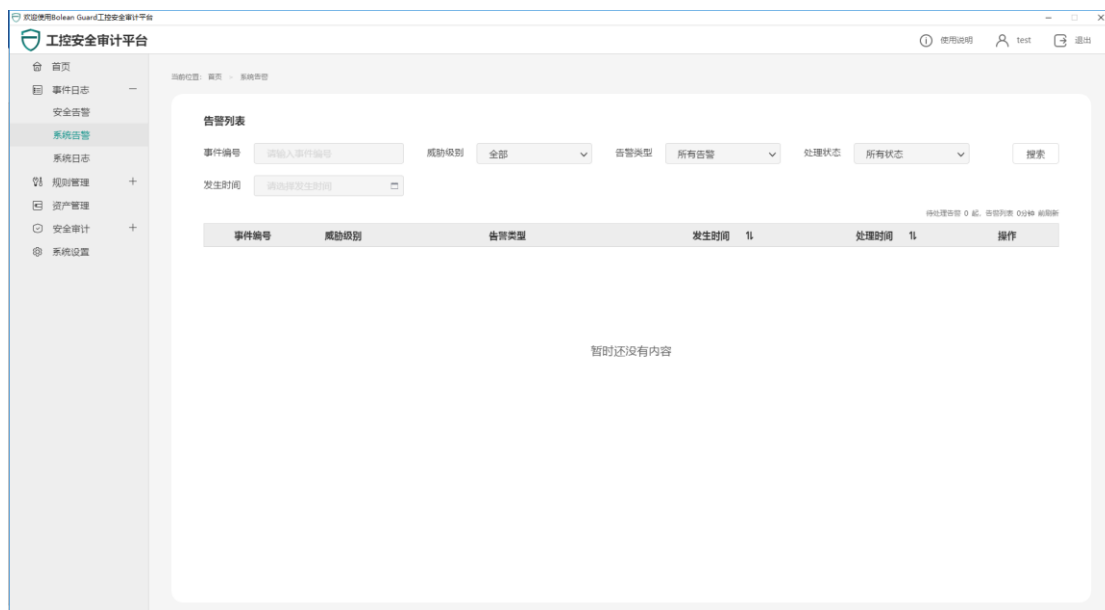


图 6-3 系统告警列表

6.3. 系统日志

系统日志主要包括用户在平台中进行操作产生的各类记录文件，如登录登出、规则变更等。

工控安全审计平台

日志列表

日志编号: 请输入日志编号 日志类型: 所有日志 发生时间: 请选择发生时间 处理状态: 所有状态 搜索

待处理告警 248 起, 查看列表 1分钟 刷新

日志编号	日志类型	IP地址	描述	发生时间 1s	处理时间 1s	操作
279	登录退出	192.168.166.133	登录审计平台成功	2018-05-21 17:09:06	未处理	查看详情
278	登录退出	192.168.166.197	登录审计平台成功	2018-05-21 17:09:05	未处理	查看详情
277	登录退出	192.168.166.133	长时间无操作自动退出	2018-05-21 17:08:58	未处理	查看详情
276	登录退出	192.168.166.197	登录审计平台成功	2018-05-21 17:08:41	未处理	查看详情
275	登录退出	192.168.166.197	登录审计平台成功	2018-05-21 17:07:32	未处理	查看详情
274	登录退出	192.168.166.197	登录审计平台成功	2018-05-21 17:02:25	未处理	查看详情
273	登录退出	192.168.166.197	登录审计平台成功	2018-05-21 17:00:34	未处理	查看详情
272	登录退出	192.168.166.197	登录审计平台成功	2018-05-21 17:00:31	未处理	查看详情
271	登录退出	192.168.166.197	登录审计平台成功	2018-05-21 16:59:24	未处理	查看详情
270	规则变更	192.168.166.197	修改编号为3的设备成功	2018-05-21 16:58:43	未处理	查看详情

1 2 3 ... 25 跳至 1 页

图 6-4 系统日志列表

工控安全审计平台

系统日志详情

事件编号: 314 发生时间: 2018-05-21 17:31:16 处理时间: 2018-05-21 17:31:22

日志类型	登录退出
用户	test
IP地址	192.168.166.133
描述	登录审计平台成功

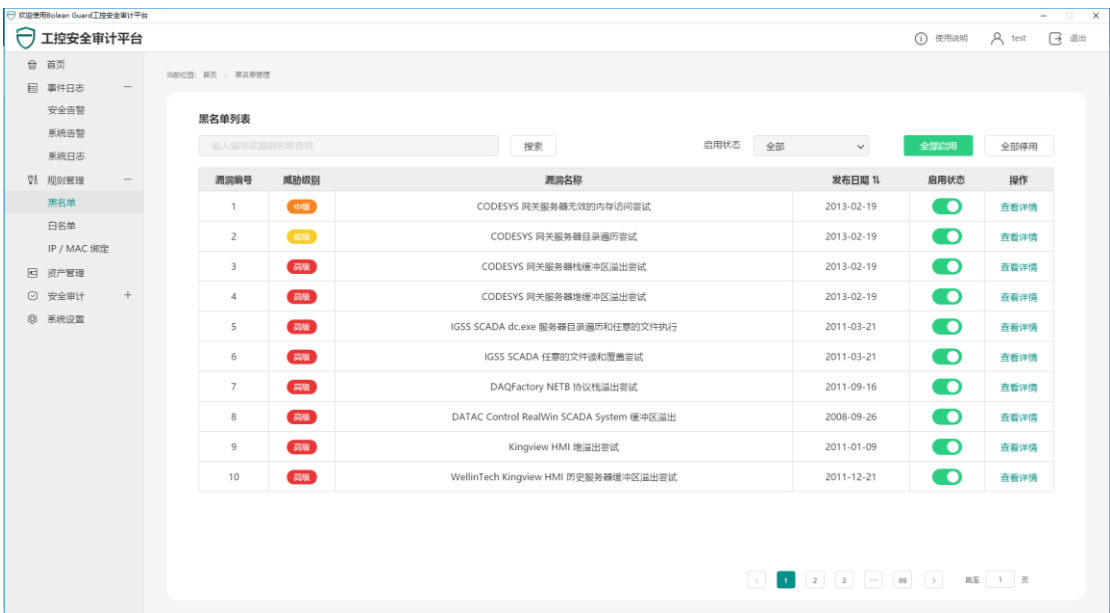
图 6-5 系统日志列表

7.规则管理

7.1. 黑名单

黑名单中包含了各种工控设备、网络设备所含有的各种可以利用、被攻击的漏洞。黑名单中的漏洞都带有特征码，从特征码可以导出预防攻击的安全保护规则。黑名单是一个长期挖掘、收集、研发、积累的过程。

黑名单页面中，可对系统中所有漏洞进行编辑。点击“启用所有”把全部漏洞部署到网络中去，点击“禁止所有”停用全部漏洞，也可以操作“启用状态”开关，对特定漏洞进行部署。



漏洞编号	威胁级别	漏洞名称	发布日期	启用状态	操作
1	中危	CODESYS 网关服务器无效的内存访问尝试	2013-02-19	<input checked="" type="checkbox"/>	查看详情
2	低危	CODESYS 网关服务器目录遍历尝试	2013-02-19	<input checked="" type="checkbox"/>	查看详情
3	高危	CODESYS 网关服务器缓冲区溢出尝试	2013-02-19	<input checked="" type="checkbox"/>	查看详情
4	高危	CODESYS 网关服务器堆缓冲区溢出尝试	2013-02-19	<input checked="" type="checkbox"/>	查看详情
5	高危	IGSS SCADA dc.exe 服务器目录遍历和任意的文件执行	2011-03-21	<input checked="" type="checkbox"/>	查看详情
6	高危	IGSS SCADA 任意的文件读和覆盖尝试	2011-03-21	<input checked="" type="checkbox"/>	查看详情
7	高危	DAQFactory NETB 协议栈溢出尝试	2011-09-16	<input checked="" type="checkbox"/>	查看详情
8	高危	DATAControl RealWin SCADA System 缓冲区溢出	2008-09-26	<input checked="" type="checkbox"/>	查看详情
9	高危	Kingview HMI 堆溢出尝试	2011-01-09	<input checked="" type="checkbox"/>	查看详情
10	高危	WellinTech Kingview HMI 历史服务器缓冲区溢出尝试	2011-12-21	<input checked="" type="checkbox"/>	查看详情

图 7-1 黑名单列表

点击相应漏洞条目内容栏的“详情”，可查看该漏洞的信息及修补特征。

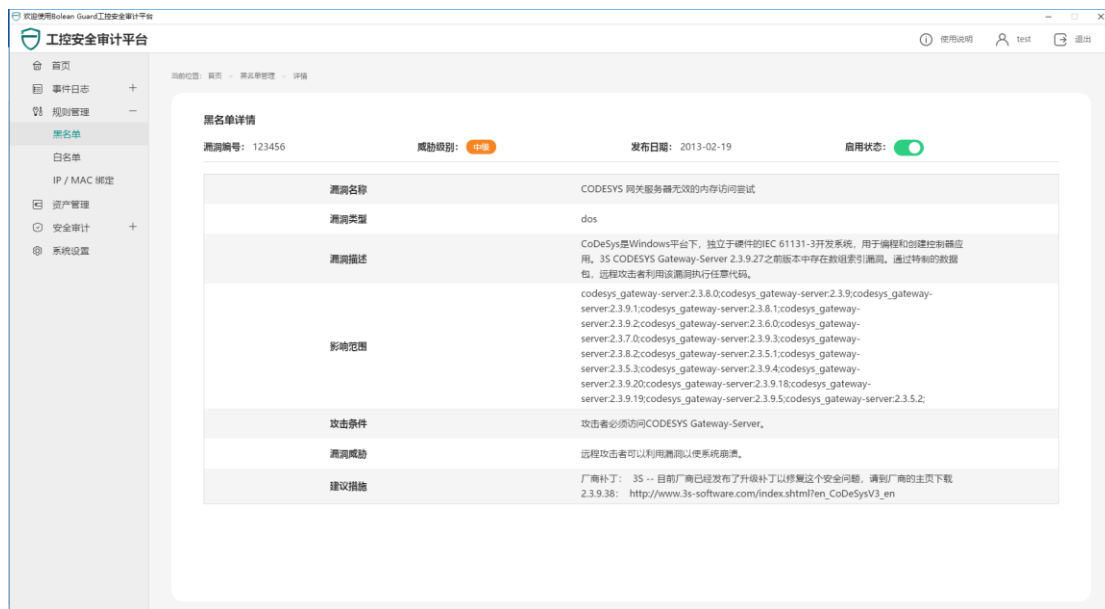


图 7-2 黑名单详情

7.2. 白名单

用户可在此新增白名单，对已有白名单规则进行编辑或删除操作。点击“全部启用”把全部白名单规则部署到网络中去，点击“全部停用”停用全部规则。也可以单独操作“启用状态”开关，对特定白名单规则进行部署。

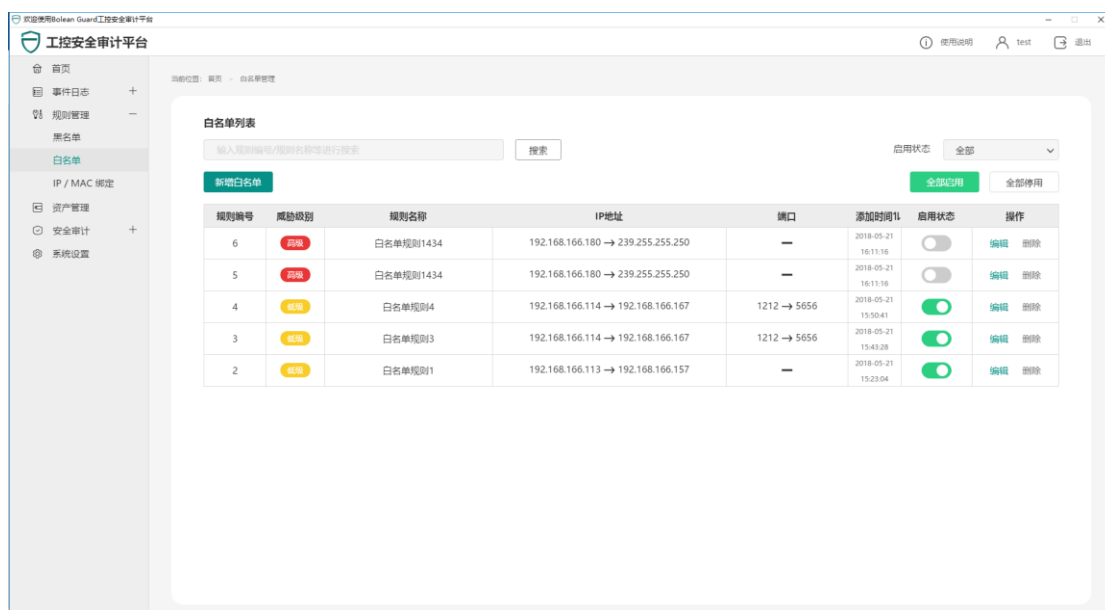


图 7-3 白名单列表

点击某条白名单对应的“编辑”按钮，该条白名单进入编辑状态，可对白名单规则内容进行修改。修改完成后，需点击“保存”按钮，所做修改方可生效。放弃修改，可点击“取消”按钮。如图所示。

自动生成	高级 ▾	白名单规则1434	192.168.166.18(→ 239.255.255.25(源端口 → 目标端	自动生成	<input checked="" type="checkbox"/>	保存	取消
------	------	-----------	-----------------------------------	-----------	------	-------------------------------------	----	----

图 7-4 编辑白名单

当有白名单规则处于正在编辑状态时，用户不可以进行其他操作。必须先保存或取消当前编辑，才可以进行其他操作。

点击某条白名单对应的“删除”按钮，弹出确认对话框，可删除该条白名单。

点击“新增白名单”按钮，在列表中第一行为输入框，如图所示。按照提示填写表单后，点击“保存”按钮，弹出成功提示，则白名单规则新增成功。

新增白名单

全部启用

全部停用

规则编号	威胁级别	规则名称	IP地址		端口	添加时间	启用状态	操作
自动生成	低级	白名单规则7	源IP	→	目标IP	源端口 → 目标端	自动生成	<div><div></div></div> <div>保存</div> <div>取消</div>

图 7-5 新增白名单

新增或编辑白名单时，填写表单规则如下。

- 规则编号：不需要填写，由系统自动生成。
- 威胁级别：默认为低级，有中、高级可选。
- 规则名称：系统会按规则顺序自动生成，用户也可以自定义填写。
- IP 地址：需要用户手动输入起始 IP 和目的 IP。
- 端口：需要用户手动输入起始端口和目的端口。
- 添加时间：不需要填写，由系统自动生成。
- 启用状态：白名单规则默认关闭的，可点击开启。

7.3. IP/Mac 绑定

IP/MAC 绑定的主要功能是添加 IP/MAC 规则，部署 IP/MAC 规则，同时添加的 IP/MAC

信息会作为白名单学习的基础。规则列表中的数据和资产管理列表同步，如图所示。

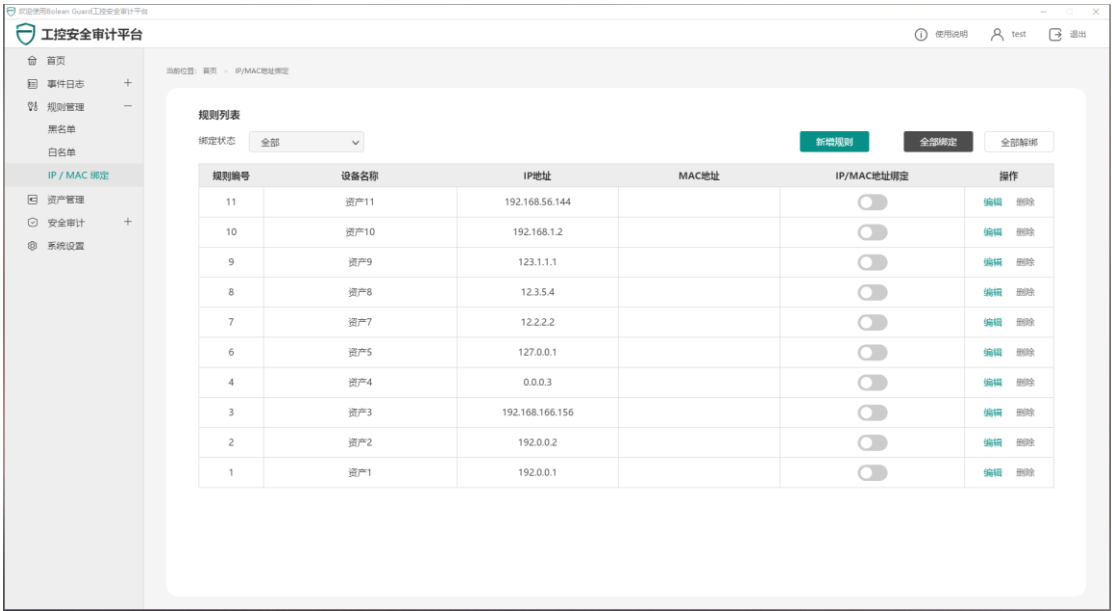


图 7-6 IP/MAC 绑定规则列表

点击某条绑定规则对应的“编辑”按钮，该条绑定规则进入编辑状态，可对绑定规则内容进行修改。修改完成后，需点击“保存”按钮，所做修改方可生效。放弃修改，可点击“取消”按钮。如图所示。

规则编号	设备名称	IP地址	MAC地址	IP/MAC地址绑定	操作
自动生成	资产23	192.168.1.1	请输入Mac地址	<input type="checkbox"/>	<button>保存</button> <button>取消</button>

图 7-7 编辑 IP/MAC 绑定规则

当有绑定规则处于正在编辑状态时，用户不可以进行其他操作。必须先保存或取消当前编辑，才可以进行其他操作。

点击某条绑定规则对应的“删除”按钮，弹出确认对话框，可删除该条绑定规则。

点击“新增规则”按钮，在列表中第一行为输入框，如图所示。按照提示填写表单后，点击“保存”按钮，弹出成功提示，则白名单规则新增成功。

规则编号	设备名称	IP地址	MAC地址	IP/MAC地址绑定	操作
自动生成	资产24	请输入IP地址	请输入Mac地址	<input type="checkbox"/>	<button>保存</button> <button>取消</button>

图 7-8 新增 IP/MAC 绑定规则

新增或编辑绑定规则时，填写表单规则如下。

- 规则编号：不需要填写，由系统自动生成。
- 设备名称：系统会按规则顺序自动生成，用户也可以自定义填写。
- IP 地址：需要用户手动输入设备 IP 地址。
- Mac 地址：需要用户手动输入设备 Mac 地址。
- 启用状态：规则默认关闭的，可点击开启。

8. 资产管理

用户可将工控网络中的设备添加到资产列表中进行管理的同时，同步部署 IP/MAC 绑定规则。

点击“添加资产”按钮，在列表中第一行出现输入框，如图所示。按照提示填写表单后，点击“保存”按钮，弹出成功提示，则新资产新增成功。

设备编号	设备名称	设备类型	IP地址	MAC地址	IP/MAC地址绑定	设备价值	备注	添加时间	操作
自动生成	资产1	通讯设备 ▼	请输入IP地址	请输入Mac地址	<input type="checkbox"/>	低 ▼	请输入备注	自动生成	<button>保存</button> <button>取消</button>

图 8-1 新增资产

点击某条资产对应的“编辑”按钮，该条资产进入编辑状态，可对资产内容进行修改。修改完成后，需点击“保存”按钮，所做修改方可生效。放弃修改，可点击“取消”按钮。如图所示。

设备编号	设备名称	设备类型	IP地址	MAC地址	IP/MAC地址绑定	设备价值	备注	添加时间	操作
自动生成	资产1	通讯设备 ▼	192.168.1.1	请输入Mac地址	<input type="checkbox"/>	中 ▼	请输入备注	自动生成	<button>保存</button> <button>取消</button>

图 8-2 编辑资产

新增或编辑资产时，填写表单规则如下。

- 规则编号：不需要填写，由系统自动生成。
- 设备名称：系统会按规则顺序自动生成，用户也可以自定义填写。
- 设备类型：可选通讯设备、控制设备、安全设备、监控设备、HMI、服务器、其他设备等。
- IP 地址：需要用户手动输入设备 IP 地址。

- Mac 地址：需要用户手动输入设备 Mac 地址。
- 启用状态：规则默认关闭的，可点击开启。
- 设备价值：可选高、中、低三种。
- 备注：对设备进行备注。
- 添加时间：不需要填写，由系统自动生成。

当有资产处于正在编辑状态时，用户不可以进行其他操作。必须先保存或取消当前编辑，才可以进行其他操作。

点击某条绑定规则对应的“删除”按钮，弹出确认对话框，可删除该条绑定规则。



图 8-3 删除资产确认

9.安全审计

9.1. 协议审计

页面上方可根据 IP、MAC、端口、起始时间以及协议类型对所有协议进行筛选。

规则列表

事件编号	<input type="text" value="请输入事件编号"/>	协议类型	<input type="text" value="请输入协议类型"/>	起始时间	<input type="text" value="请选择起始时间"/>	<input type="button" value="搜索"/>
IP地址	<input type="text" value="请输入IP地址"/>	MAC地址	<input type="text" value="请输入MAC地址"/>	端口	<input type="text" value="请输入端口"/>	

图 9-1 协议筛选

审计结果列表显示协议的起始时间、IP 地址、MAC 地址、端口以及协议类型。

图 9-2

点击协议条目栏的“详情”，可查看该协议的详细信息。

图 9-3

9.2. 流量审计

展示一段时间内的流量状态。

10. 系统设置

系统设置页面分为基础设置和高级设置。

10.1. 基础设置

“基础设置”标签显示当前连接的设备 IP 地址、时间及基础信息。如图所示。

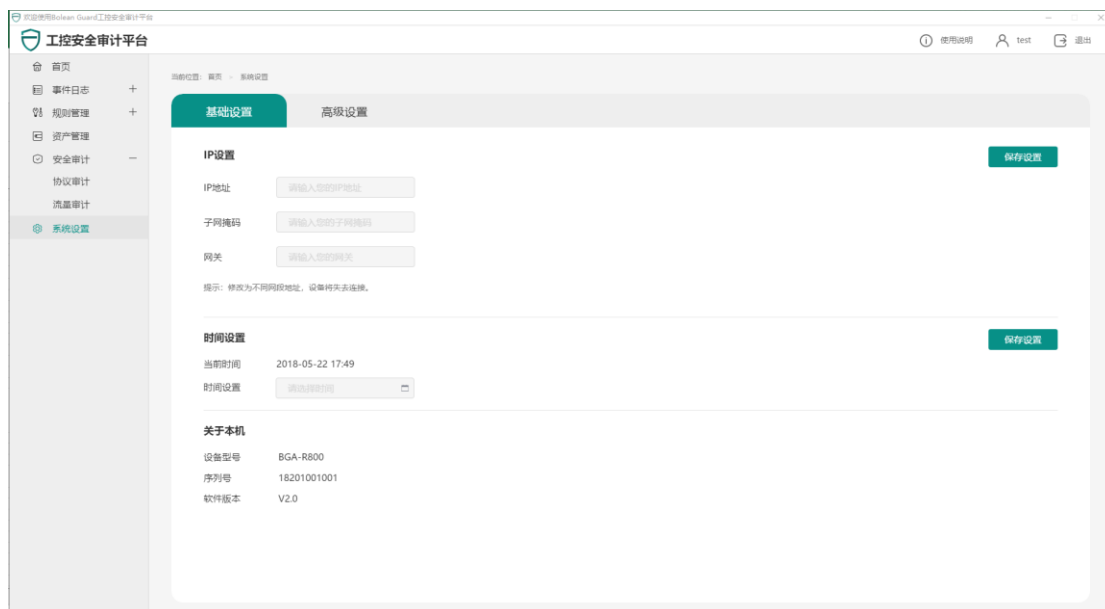


图 10-1 基础设置

“IP 设置”模块显示当前连接设备的 IP 信息，同时提供设置 IP 的功能。按提示输入 IP、子网掩码和网关后，点击“保存设置”按钮，页面将自动跳转到登录界面，重新登录目标设备。

“时间设置”模块用户需要手工输入时间。编辑完成后点击对应的“保存设置”按钮，修改即生效。

“关于本机”模块展示当前设备型号、序列号、软件版本等信息。

10.2. 高级设置

10.2.1. 系统重置

该模块展示设备本次启动时间及运行时长。点击“重新启动”按钮，输入当前账户密码验证身份。成功后弹出重启提示，设备进行重启。重启完成后，用户需要重新登录。

系统重置

本次运行	0天1小时23分
本次开机时间	2018-05-22 16:26:43

重新启动



10.2.2. 登录安全

“登录安全”模块可设置当前设备的系统强制登出时间、用户可尝试登录次数以及失败后

账号锁定时间。

登录安全

无操作自动退出 分钟
密码输入错误锁定 次
账号锁定时长 分钟

保存设置

10.2.3. 远程登录

此模块可设置允许所有用户 IP 登录或仅允许特定用户 IP 登录。默认为“允许所有 IP”登录审计平台，点击可切换至“仅允许特定 IP”登录审计平台。

远程登录设置

IP远程登录

☒ 允许所有IP

☐ 仅允许特定IP

保存修改

若需设置特定 IP 才能登录审计平台时，请按以下步骤操作：

1. 点选“仅允许特定 IP”，弹出允许远程登录的 IP 输入框。

远程登录设置

IP远程登录

☐ 允许所有IP

☒ 仅允许特定IP

保存修改

允许远程登录的IP

输入IP地址，多个IP用逗号隔开

添加到列表

允许远程登录的IP	操作

2. 输入允许登录该设备的 IP 地址，点击“添加到列表”按钮。输入的 IP 地址出现在下方的表格中。

允许远程登录的IP

添加到列表

允许远程登录的IP	操作
192.18.1.1	删除

3. 点击“保存修改”按钮，弹出提示，则允许远程登录的 IP 添加完成。

✓ 远程登录设置成功

11. 设备维护及常见问题处理

11.1. 故障诊断

智能监测审计平台出现故障时，查看面板上的 LED 指示灯或客户端的日志记录，可对故障进行处理。

11.2. 故障处理

本使用手册只介绍简单的故障处理方法，如仍不能排除，请联系木链科技寻求技术支持。

以下为故障处理方法：

Power 灯不亮	请检查电源线连接是否正确。
	请检查电源线正负极（DC）或零、火是否接反。
	请检查电源线插头是否插紧。
	请检查电源电压是否符合要求。
MGMT 端口灯不亮	请检查连接 MGMT 端口的设备或交换机是否启动。
	请检查连接 MGMT 端口的网线接口制作是否正确。

	请更换更好的网线。
设备失去连接	Ping 审计平台的管理 IP 地址，看是否 Ping 的通。
	把配置电脑 IP 地址与监测审计平台网管 IP 设置同一网段。