2016乌云白帽大会・不插电

威胁情报联盟

Who Am I ?

- 瞌睡龙
- 乌云合伙人、知识库负责人

威胁情报是针对已有或新型的威胁或风险采取响应的一种实证知识，
包括背景、运作机制、标识、启示性的和可操作性的建议。

— Gartner（全球最具权威的IT研究与顾问咨询公司）

我们理解的威胁情报

我们理解的威胁情报

数据安全

服务器安全

交换机安全

数据库安全

员工PC安全

等……

Web应用防火墙

IDS、IPS

端点监控

等……

我们理解的威胁情报

业务安全

DDoS攻击
CC攻击
被薅羊毛
被撞库
等……

网络防火墙
业务安全产品
自身业务数据分析
等……

我们所做的事情

数据安全

- ThreatKey蜜网监控

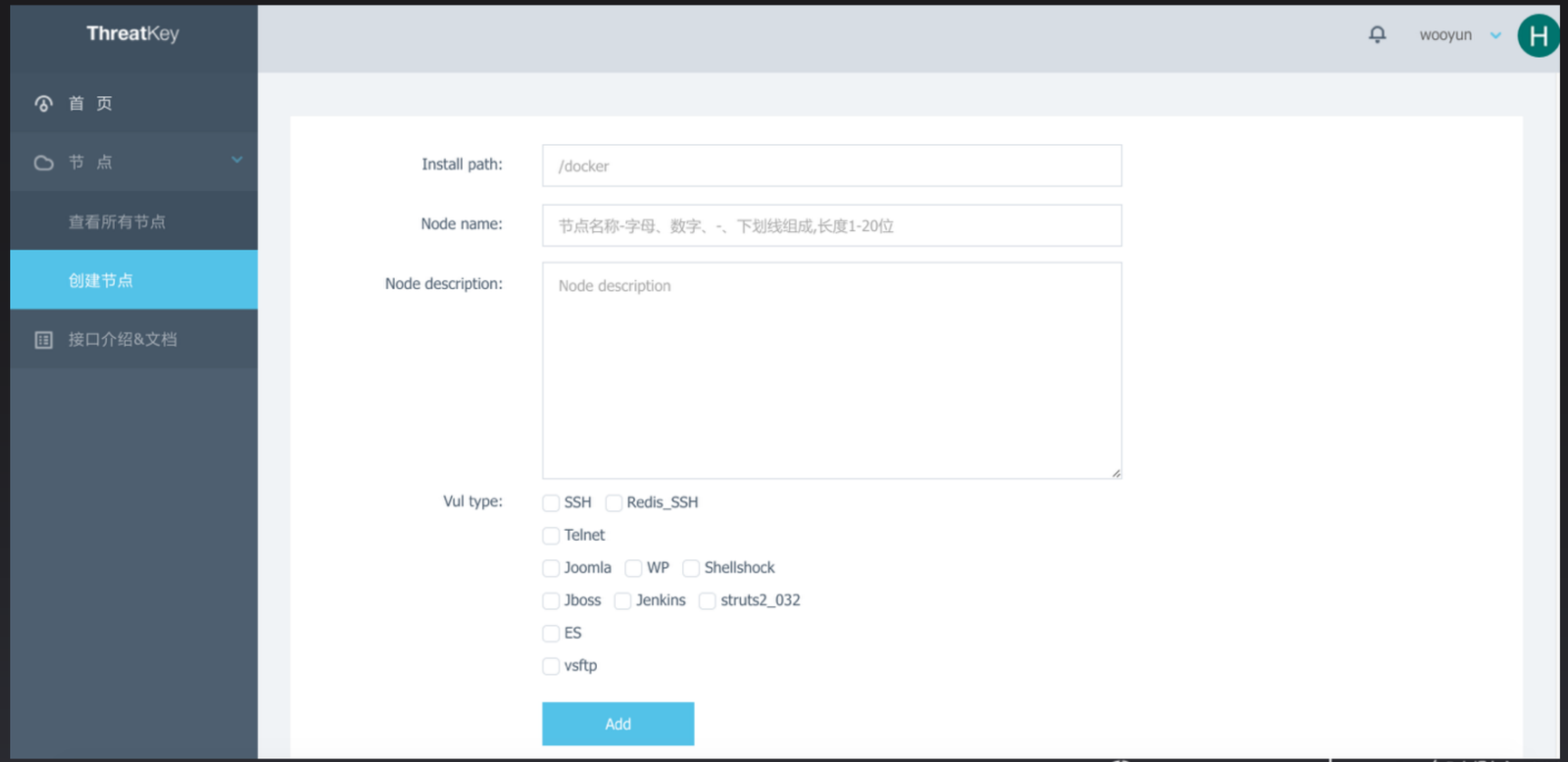
业务安全

- 互联网风控基础数据

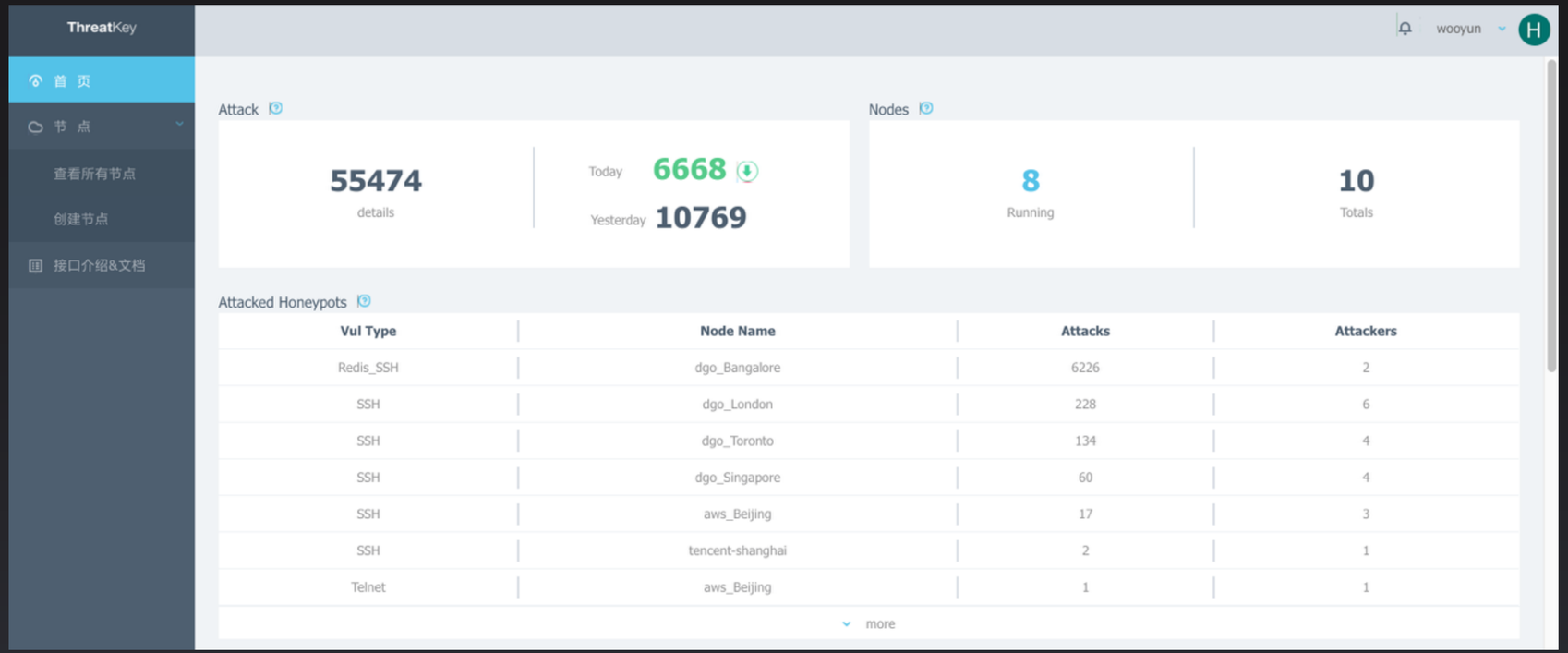
ThreatKey简介

- 基于Docker的高交互蜜罐系统
- 部署脚本一键安装
- 蜜罐网络安全限制
- 云端直接管理蜜罐（新增、启动、重置）
- 多样化日志收集、查询、分析

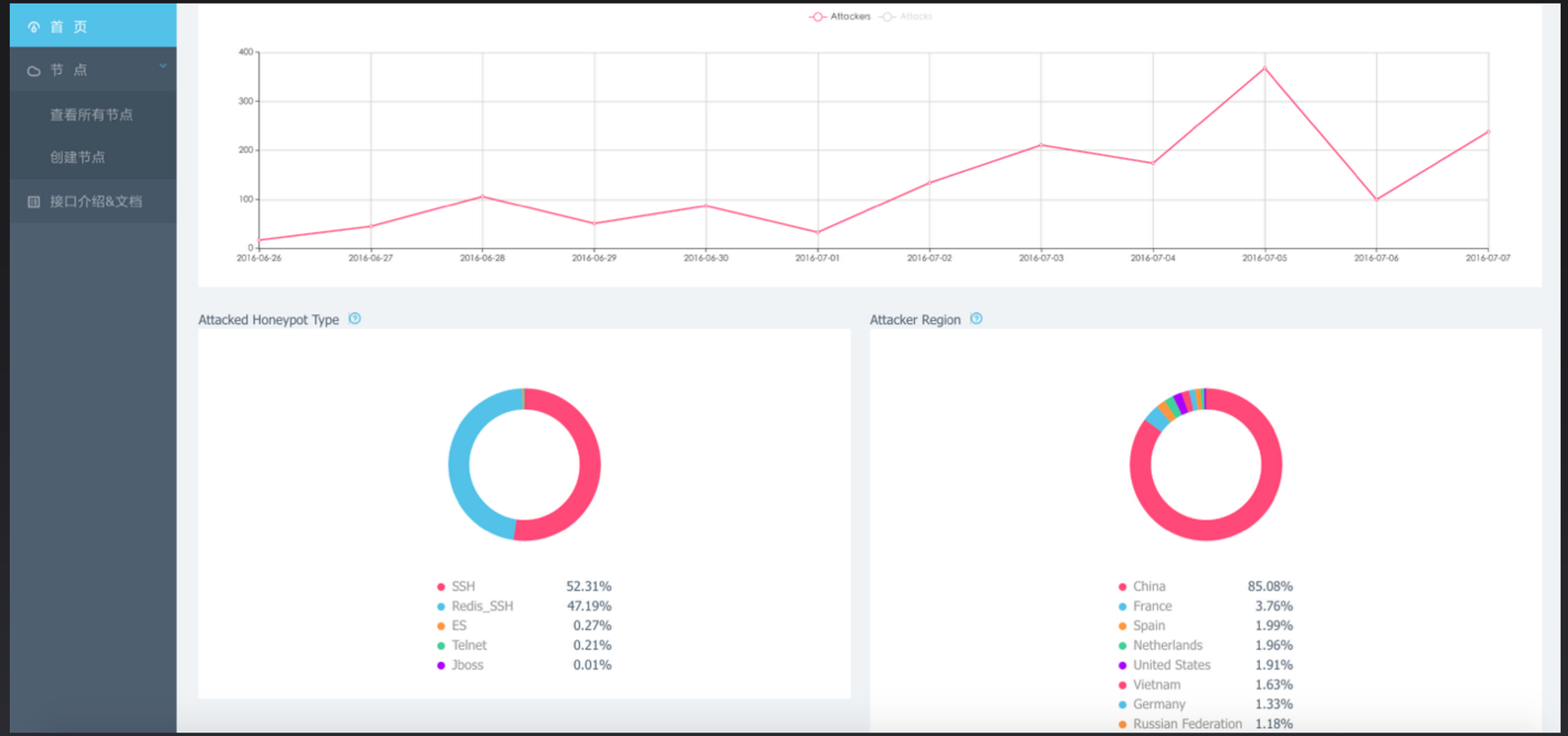
ThreatKey.com



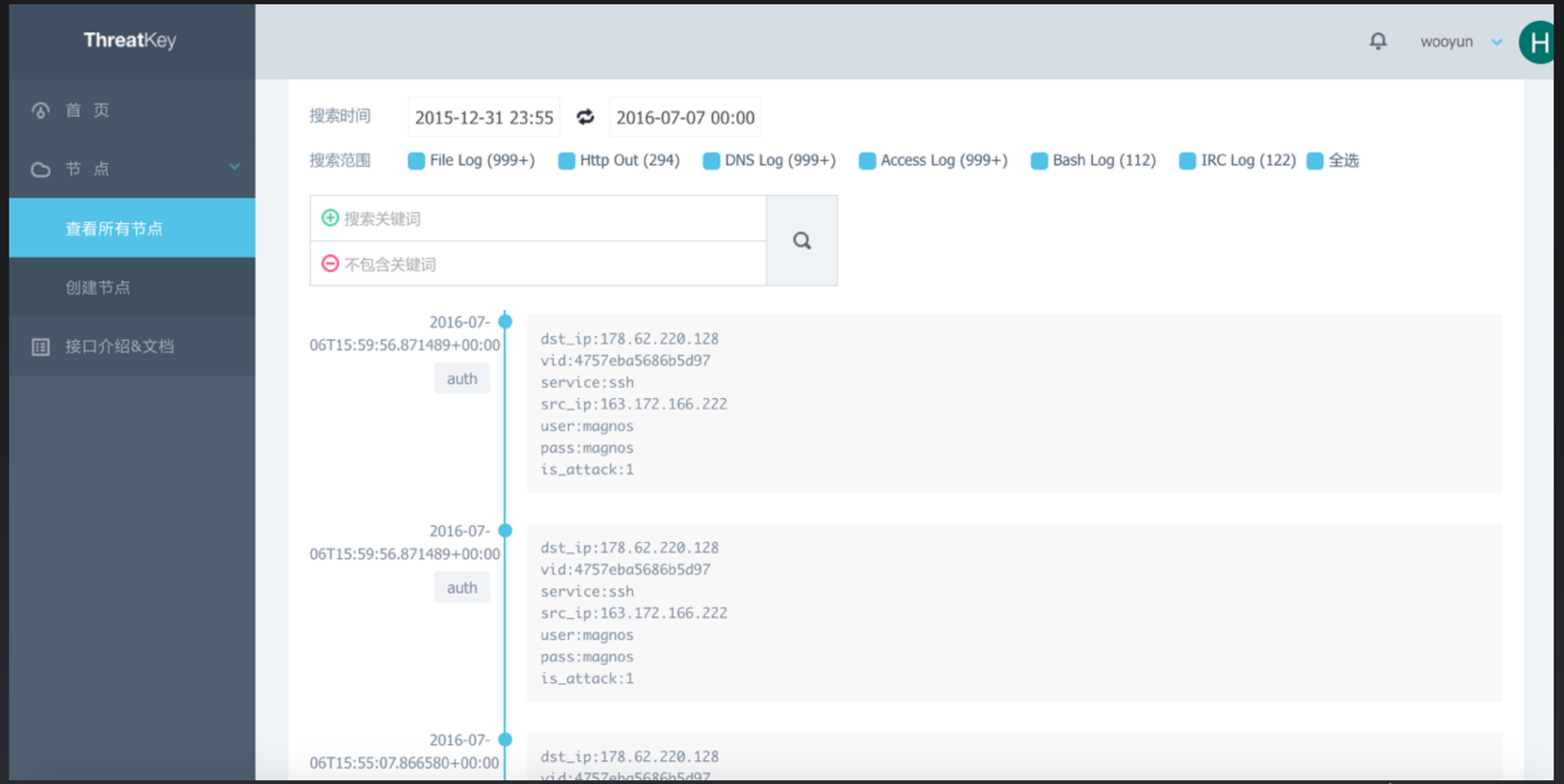
ThreatKey.com



ThreatKey.com



ThreatKey.com



互联网风控基础数据

Risk.WooYun.org

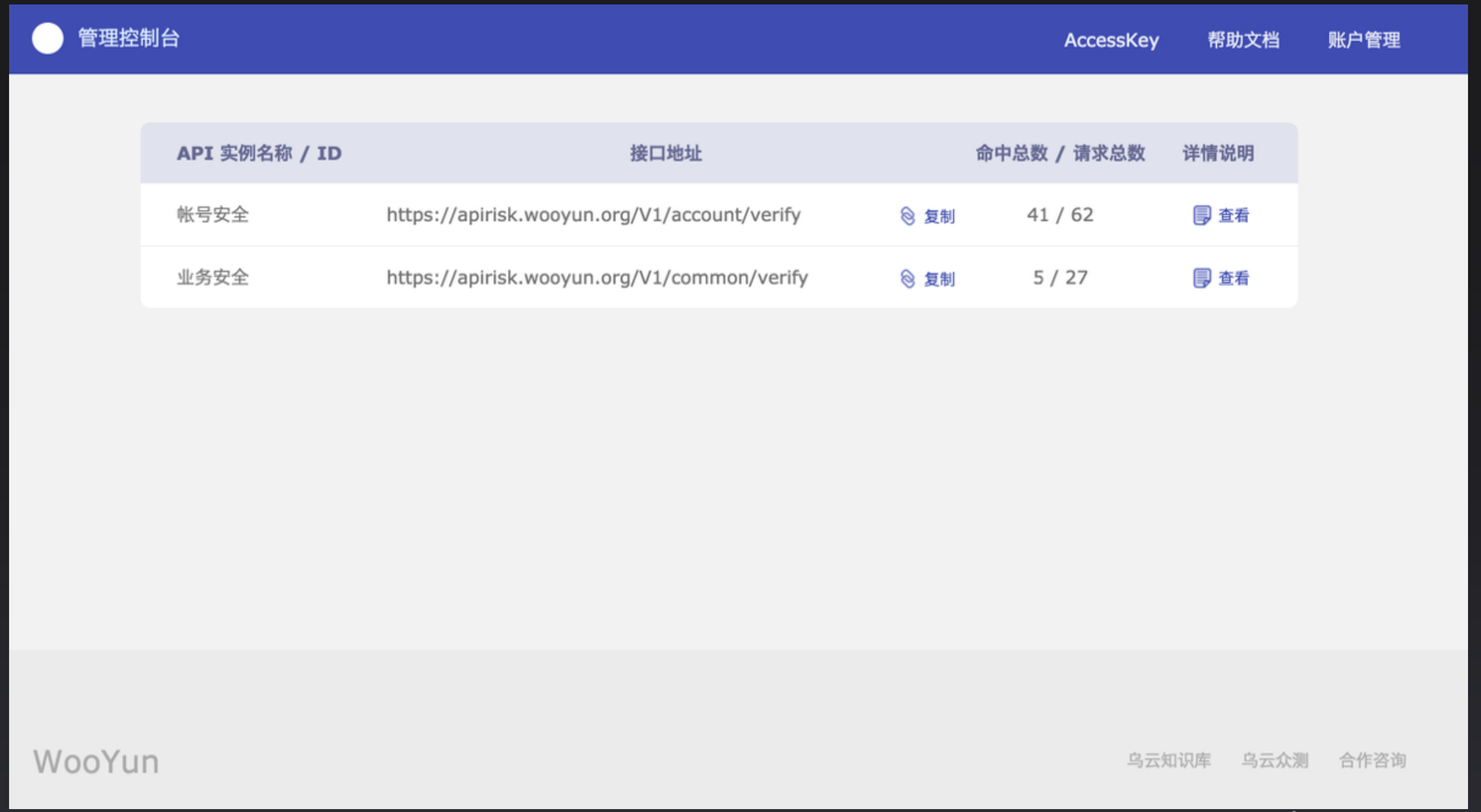
- 羊毛党手机号
- 被钓鱼银行卡号
- 代理IP地址

互联网风控基础数据

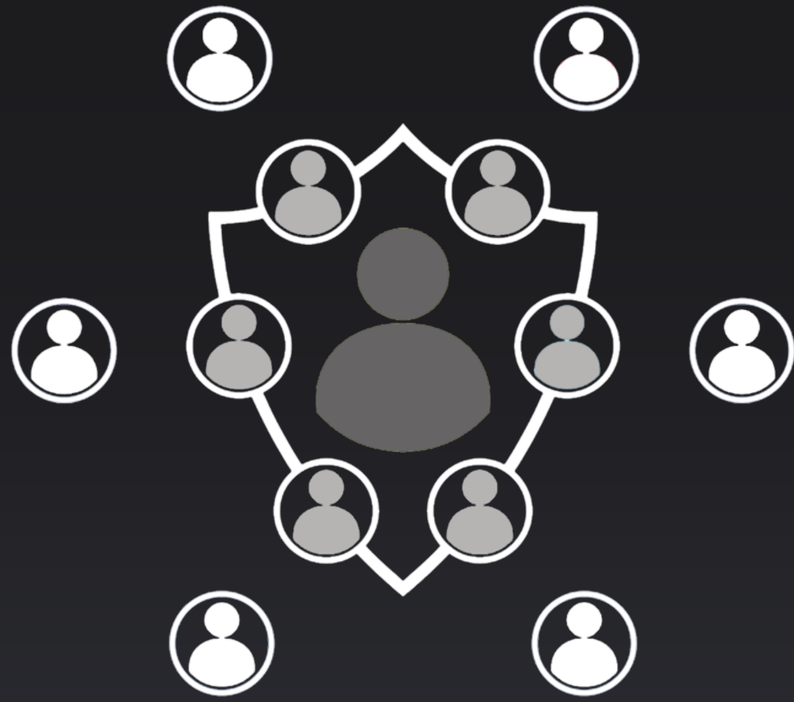
Risk.WooYun.org

互联网风控基础数据

Risk.WooYun.org



我们希望未来的安全



THANKS

乌云 WooYun

乌云白帽大会 · 2016
不插电