



WHITE HAT FEST

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**。

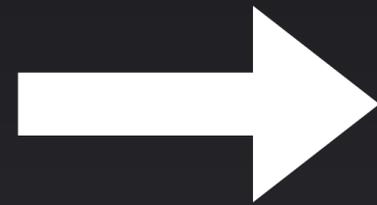
— Gartner（全球最具权威的IT研究与顾问咨询公司）

我们理解的威胁情报

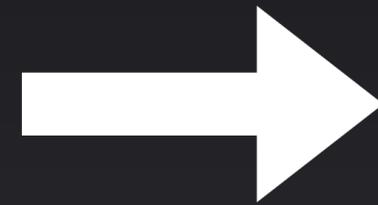


我们理解的威胁情报

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

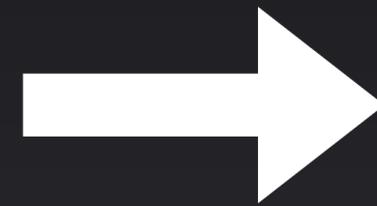
IDS、IPS

endpoint 监控

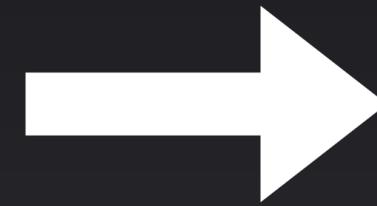
等.....

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

首页

节点

查看所有节点

创建节点

接口介绍&文档

Install path: /docker

Node name: 节点名称-字母、数字、-、下划线组成,长度1-20位

Node description: Node description

Vul type:

- SSH
- Redis_SSH
- Telnet
- Joomla
- WP
- Shellshock
- Jboss
- Jenkins
- struts2_032
- ES
- vsftp

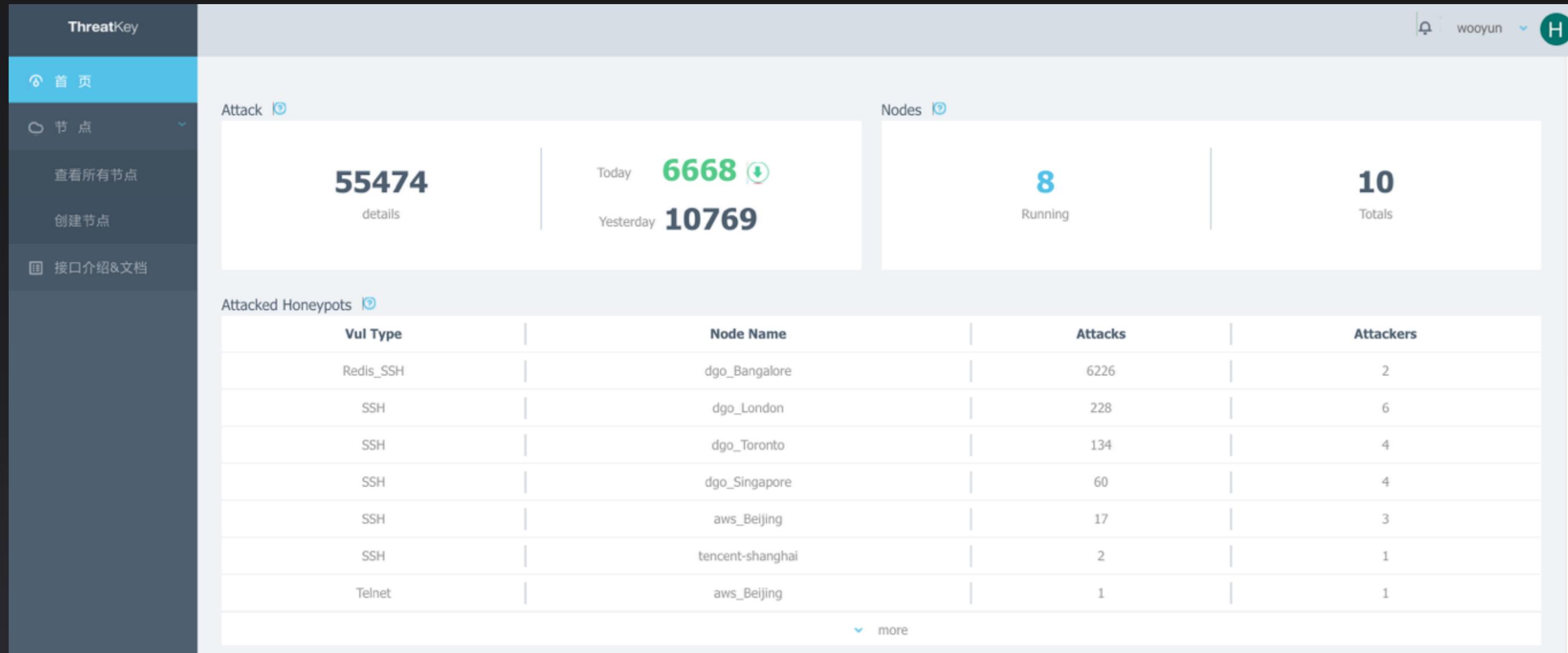
Add

wooyun

乌云 WooYun

乌云白帽大会·2016
不插电

ThreatKey.com



ThreatKey.com

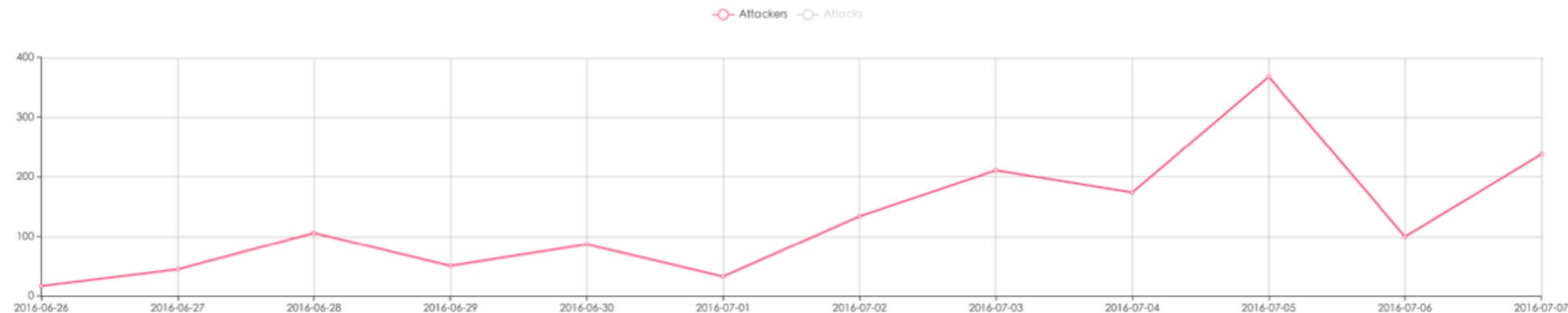
首页

节点

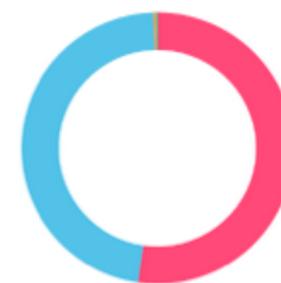
查看所有节点

创建节点

接口介绍&文档

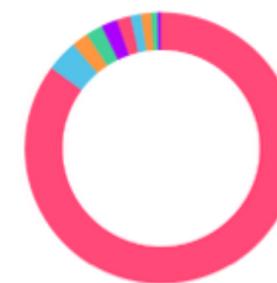


Attacked Honeypot Type



SSH	52.31%
Redis_SSH	47.19%
ES	0.27%
Telnet	0.21%
Jboss	0.01%

Attacker Region



China	85.08%
France	3.76%
Spain	1.99%
Netherlands	1.96%
United States	1.91%
Vietnam	1.63%
Germany	1.33%
Russian Federation	1.18%

ThreatKey.com

The screenshot displays the ThreatKey web interface. On the left is a dark sidebar with navigation options: 首页 (Home), 节点 (Nodes), 查看所有节点 (View all nodes), 创建节点 (Create node), and 接口介绍&文档 (API Introduction & Docs). The main content area features a search interface with the following elements:

- 搜索时间 (Search Time):** 2015-12-31 23:55 to 2016-07-07 00:00
- 搜索范围 (Search Scope):** File Log (999+), Http Out (294), DNS Log (999+), Access Log (999+), Bash Log (112), IRC Log (122), 全选 (Select All)
- 搜索关键词 (Search Keywords):** A search bar with a magnifying glass icon.
- 不包含关键词 (Exclude Keywords):** A search bar with a minus sign icon.

Below the search filters, a vertical timeline shows log entries for authentication attempts:

- 2016-07-06T15:59:56.871489+00:00:** auth. Metadata: dst_ip:178.62.220.128, vid:4757eba5686b5d97, service:ssh, src_ip:163.172.166.222, user:magnos, pass:magnos, is_attack:1.
- 2016-07-06T15:59:56.871489+00:00:** auth. Metadata: dst_ip:178.62.220.128, vid:4757eba5686b5d97, service:ssh, src_ip:163.172.166.222, user:magnos, pass:magnos, is_attack:1.
- 2016-07-06T15:55:07.866580+00:00:** Metadata: dst_ip:178.62.220.128, vid:4757eba5686b5d97.

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

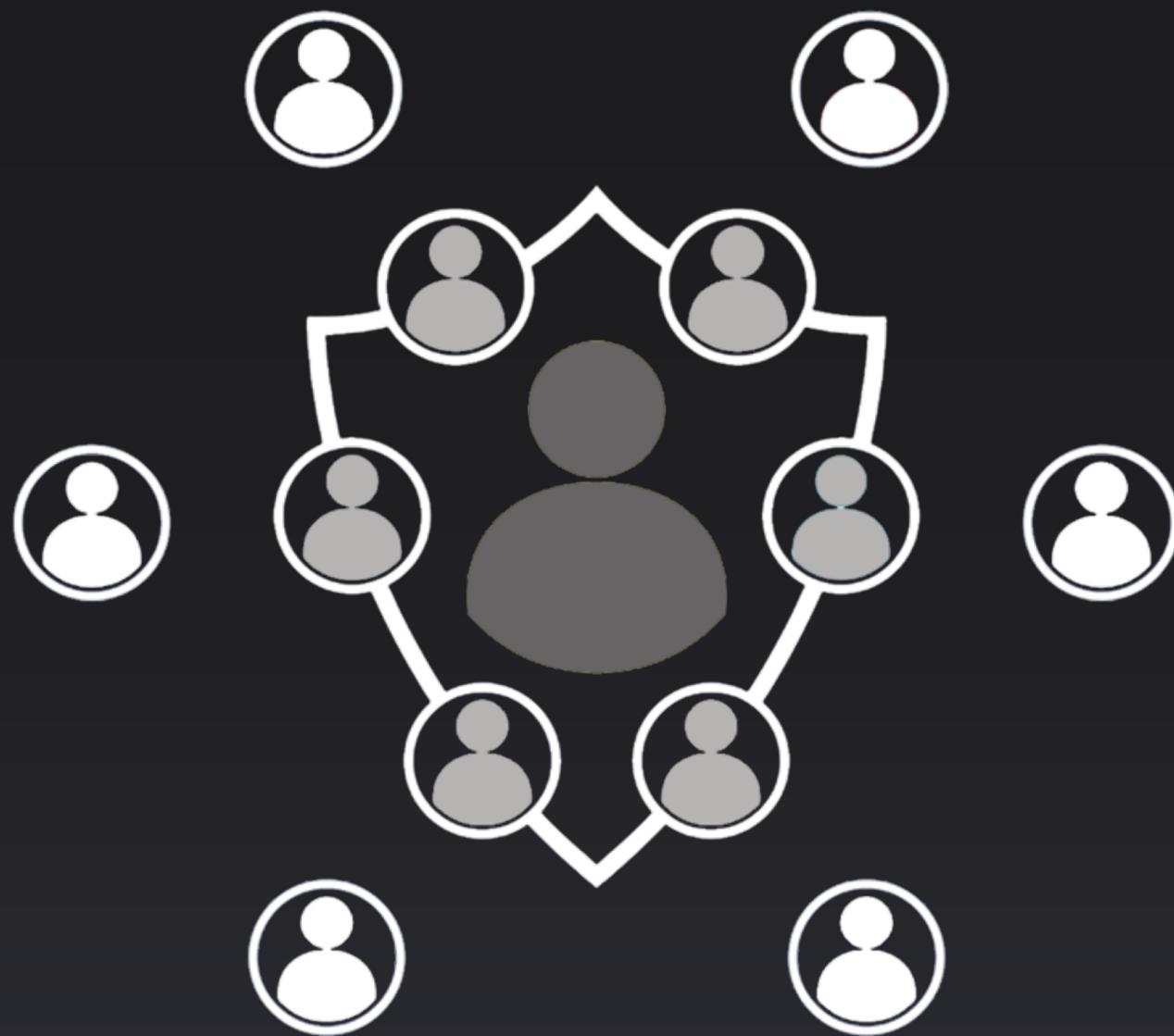
Risk.WooYun.org

管理控制台 AccessKey 帮助文档 账户管理

API 实例名称 / ID	接口地址		命中总数 / 请求总数	详情说明
帐号安全	https://apirisk.wooyun.org/V1/account/verify	复制	41 / 62	查看
业务安全	https://apirisk.wooyun.org/V1/common/verify	复制	5 / 27	查看

WooYun 乌云知识库 乌云众测 合作咨询

我们希望未来的安全



THANKS



乌云 WooYun



乌云白帽大会 · 2016
不插电