

谛听 D-Sensor 使用说明

事件分析

事件分析

1. 点击事件分析跳转至事件分析界面，上半部分为事件分析列表筛选，下半部分为事件列表。

事件分析

您好, 系统管理员, 今天是 2017 年 09 月 14 日

选择节点: 所有节点

事件类型: 异常行为

选择时间, 留空则搜索所有事件

重置 搜索

节点	攻击 IP	事件	开始时间	结束时间
wiki	192.168.12.1	action	2017-09-11 18:35:58	2017-09-11 18:35:58

D-Sensor© Chaitin Tech.

事件列表展示

2. 点击事件列表中事件，可以展开事件，并以时间轴的方式由上至下依次显示。

事件分析

您好, 系统管理员, 今天是 2017 年 09 月 14 日

选择节点: 所有节点

事件类型: 异常行为

选择时间, 留空则搜索所有事件

重置 搜索

节点	攻击 IP	事件	开始时间	结束时间
wiki	192.168.12.1	action	2017-09-11 18:35:58	2017-09-11 18:35:58

wiki 节点事件时间线

2017-09-11 18:35:58 ssh login [{"success":true,"username":"root","password":"123456"}]

收起

事件筛选

3.筛选部分可以通过监控节点、事件类型、触发事件进行筛选。点击搜索，事件列表中呈现筛选后的结果。

The screenshot shows the '事件分析' (Event Analysis) interface. The top navigation bar includes the '谛听' (Diting) logo and the user's name '您好, 系统管理员, 今天是 2017 年 09 月 14 日'. The left sidebar contains navigation items: '状态综述', '节点状态', '事件分析', '日志管理', '系统配置', 'Agent 配置', '节点配置', '伪装信息', 'Syslog 配置', '告警配置', and '许可证信息'. The main content area features a filter section with three input fields: '选择节点' (Set to '所有节点'), '事件类型' (Set to '操作回放'), and '选择时间, 留空则搜索所有事件'. Below these are '重置' and '搜索' buttons. The event list table below shows one event:

节点	攻击 IP	事件	开始时间	结束时间
wiki	127.0.0.1	replay	2017-09-11 18:36:03	2017-09-11 18:36:03

Below the table, a timeline titled 'wiki 节点事件时间线' shows a single event at '2017-09-11 18:36:03' with details 'ssh' and 'replay', and a '播放' (Play) button. A '收起' (Collapse) button is also present.

谢谢使用

若想体验更多安全产品和安全服务, 请联系长亭客服

长亭客服热线: 4000-327-707

长亭科技7×24小时为您的安全保驾护航