威胁情报

产品文档

文档目录

产品简介

威胁情报概述

最近更新时间: 2022-10-28 16:38:56

威胁情报聚焦多源威胁情报管理，全面提供多源情报接入、融合存储、情报生命周期管理、情报共享输出、情报生产、威胁预警、情报查询展示等能力。

为什么需要威胁情报

最近更新时间: 2022-10-28 16:38:56

现在黑客的攻击手段更加隐蔽化、复杂化、智能化。从攻击目的来看，黑客已经从最初的炫耀、破坏和窃取数据，转向以牟利为主的黑灰产业化运作为主，如僵尸网络、挖矿程序、用户数据窃取等，威胁情报会及时更新全球安全威胁动态信息，针对具有威胁的IP、URL、域名、文件、漏洞会给出详细的说明并且给出相应的解决方案。

产品优势

最近更新时间: 2022-10-28 16:38:56

让威胁全面清晰可见

威胁情报汇集不同来源的威胁情报及网络基础设施的数据，帮助企业安全人员了解最新的入侵威胁信息，包括IP、域名、URL、文件Hash等是否存在被加入黑名单、关联的域名、关联的文件、相关攻击组织等历史信息，并且会指出哪些应用、系统和用户群最有可能遭受攻击，同时会给出相应的解决方案建议，指导安全人员优先保护这些高风险目标。

准确快速响应针对性攻击

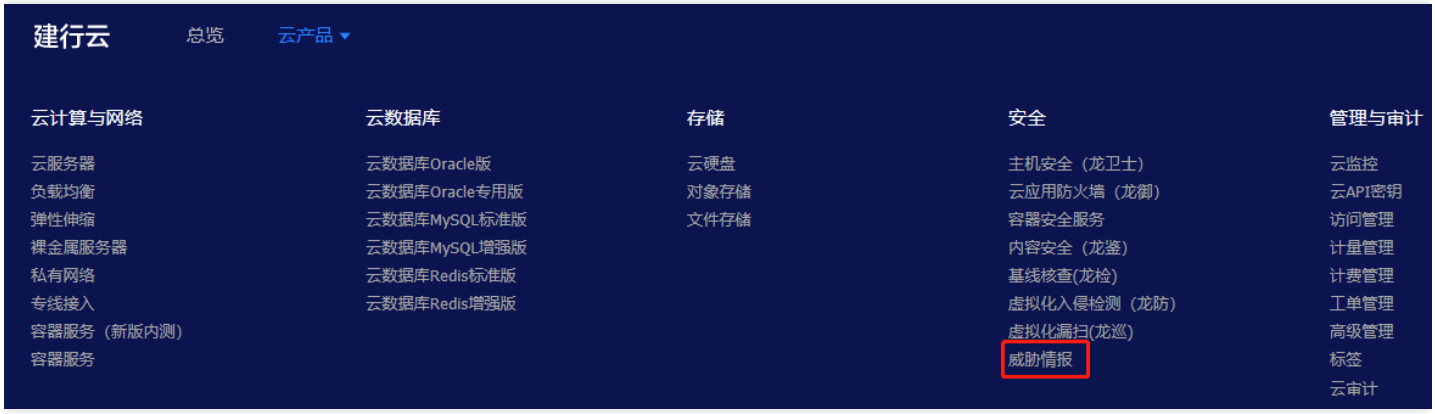
威胁情报会为客户安全团队提供详尽的信息，帮助他们了解哪些威胁最有可能影响客户所处行业及该企业本身环境，根据不同环境给出不同整改方案。 威胁情报还可帮助企业优化漏洞修复，更快速响应紧急威胁。企业不再根据“高危/重要/中危/低危”这样简单粗暴的评级，来决定应优先修复哪些漏洞，威胁情报可以为他们提供每个漏洞的详情，包括漏洞的原理、利用的难易程度以及外界是否已经出现利用方法或工具。优先次序安排得当则可以缩短对紧急威胁的响应时间，而不是浪费时间去修复一些“高危”但实际没有风险的漏洞。

快速入门

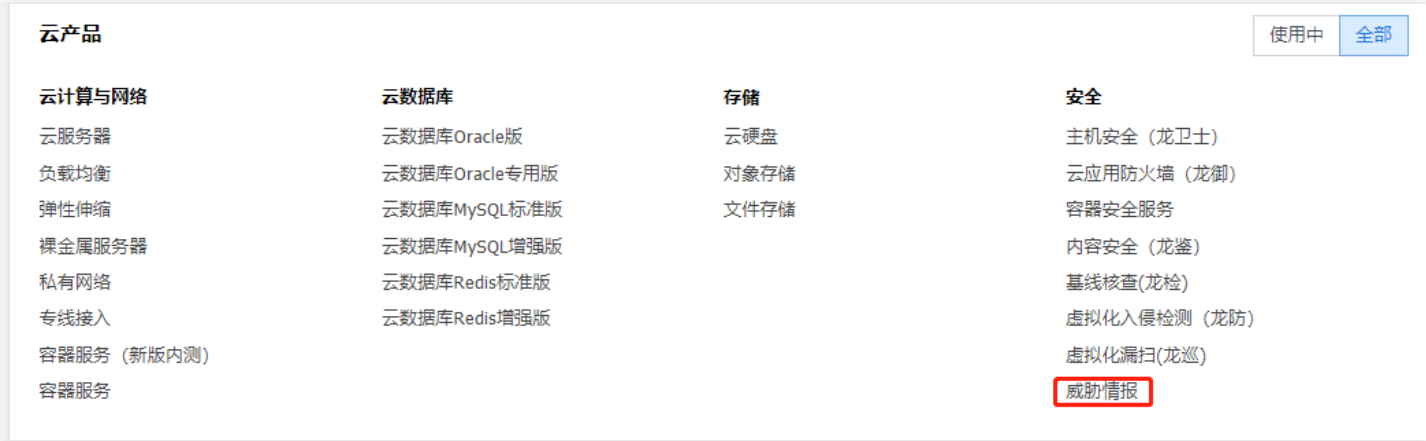
登陆威胁情报

最近更新时间: 2022-10-28 16:38:56

方式一：登录建行云平台，点击【云产品】→【安全】→【威胁情报】；

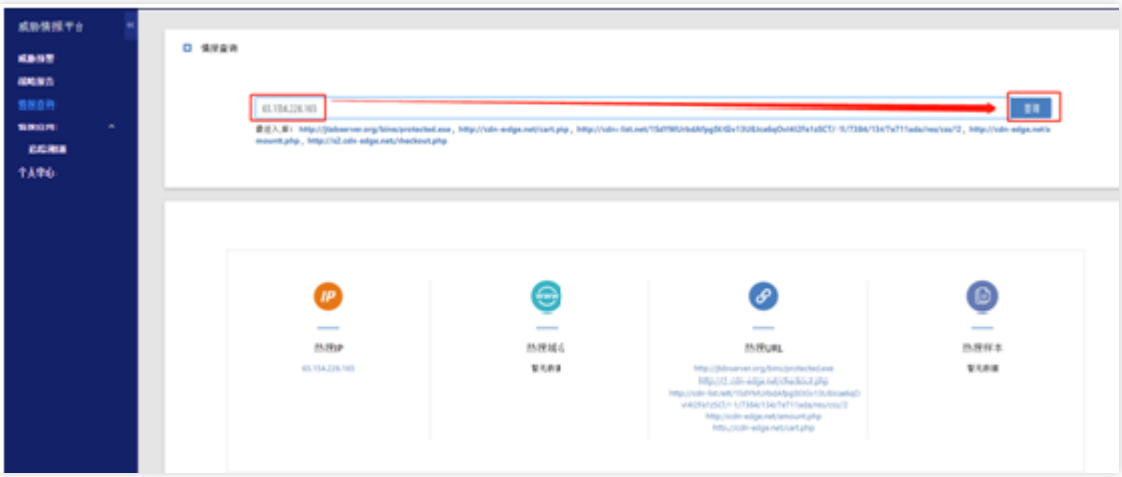


方式二：登录建行云平台，点击【总览】→【产品】→【安全】→【威胁情报】；

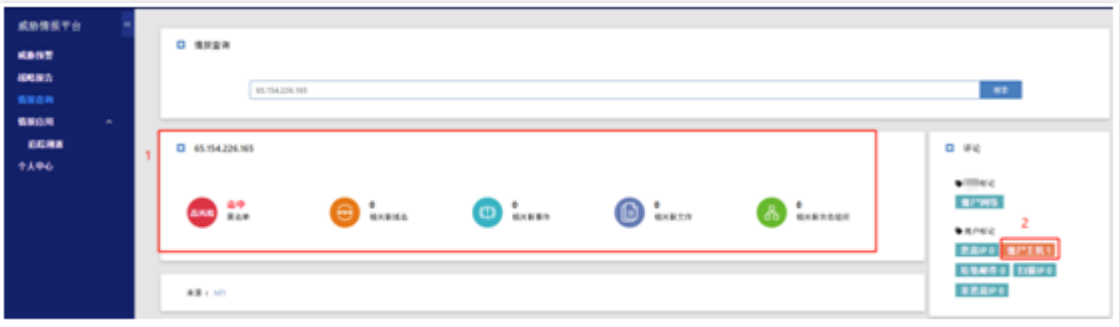


操作指南
情报查询

最近更新时间: 2022-11-08 11:04:12



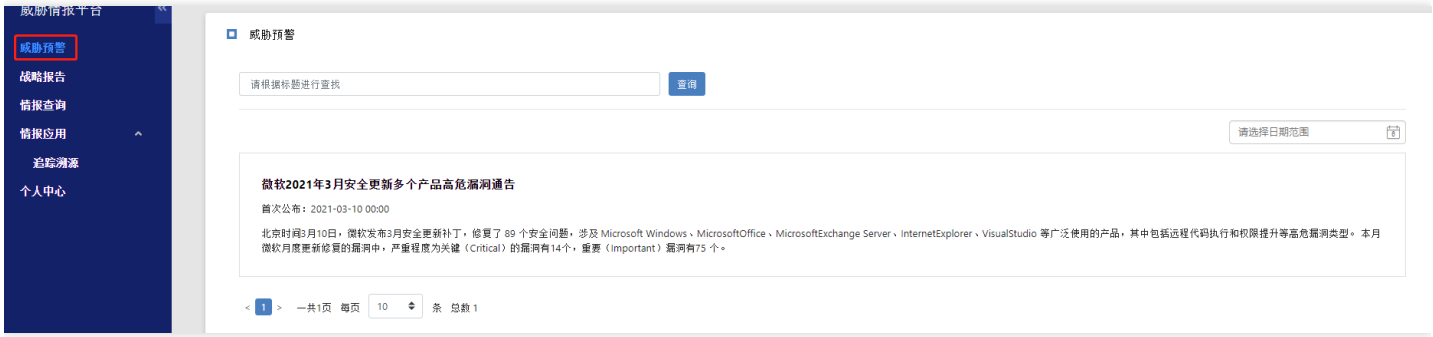
在此处输入IP、域名、URL、漏洞编号、文件Hash（MD5/SHA256/SHA1），此案例使用的为IP地址，然后点击查询



1、 可显示该IP地址是否被添加黑名单、关联的域名、关联的域名、关联的文件、使用该IP的相关攻击组织等信息
2、 可在右侧对该IP做标记，恶意IP、僵尸主机、垃圾邮件、扫描IP、非恶意IP

威胁预警

最近更新时间: 2022-10-28 16:38:56



描述业内安全事件以及热点安全漏洞的通告信息，引导用户快速响应高风险安全动态，在攻击发生前通过预先处置降低被攻击的风险。在热点漏洞或重大安全风险出现前，提供相关漏洞或事件的详细描述提醒用户预警，并提供详细的处置建议。

战略报告

最近更新时间: 2022-10-28 16:38:56

战略报告分为专题报告、威胁热点、安全研究、行业动态4种类型，并可为其加上11种（DDoS、Botnet、物联网、金融、政府、运营商、工控、漏洞、APT、周报、月报）标签，便于用户查阅。

追踪溯源

最近更新时间: 2022-11-08 11:04:12

追踪定位攻击源头，并进行可视化展示。

常见问题

情报查询关键字有哪些?

最近更新时间: 2021-10-09 14:13:39

情报查询可按IP地址、域名、URL漏洞编号、文件Hash （MD5/SHA256/SHA1）查询。

什么是追踪溯源?

最近更新时间: 2021-10-09 14:13:39

追踪溯源依托深度关联和多元分析能力，支持通过威胁指示器情报 进行追踪溯源，追踪定位攻击源头，并进行可视化展示。

什么是IOC?

最近更新时间: 2021-10-09 14:13:39

IOC的全名是Indicators of Compromise，即威胁指示器。IOC情报提供的查询为精确查询，与情报库中威胁指示器、事件、漏洞、攻击组织、攻击工具的模糊查询有所区别。

情报多久更新一次?

最近更新时间: 2021-10-09 14:13:39

情报每一小时更新一次。