奇安信
新一代网络安全领军者

奇安信威胁情报中心简介

奇安信威胁情报中心是奇安信集团旗下专门从事威胁情报领域技术研究、产品孵化的研究机构，是中国威胁情报行业领军者。致力于为国家网络安全和企业网络安全领域提供创新、领先的威胁情报能力，以完善组织的安全运营体系。

威胁情报能力服务 THREAT INTELLIGENCE CAPABILITY SERVICE

01 机读威胁情报

- 失陷检测情报
- IP信誉情报
- 文件信誉情报
- URL信誉情报
- 漏洞情报

02 人读威胁情报

- APT情报
- 安全通告报告

03 云端SaaS服务平台

威胁判定支持平台

提供多维度的威胁情报数据及分析应用，帮助安全运营者对事件报警进行确认和优先级排序，同时通过关联分析以挖掘攻击事件背后深层的信息：攻击团伙及其攻击目的、危害和历史攻击事件，是建构新型安全架构的核心组件之一。

实时威胁监控平台（威胁雷达）

基于Passive DNS数据专门为监管部门打造的一款威胁情报SaaS 应用，整合了奇安信的高、中位威胁情报能力，提供指定区域内网络威胁高位监控、案件拓线分析、样本深度分析等多种能力。

威胁分析武器库

多维度全方位便捷工具，支持快速、高效、精准的鉴别能力，协助安全运营人员对文件、网络流量、主机日志进行深度分析，输出判定结论，发现攻击痕迹，关联溯源攻击路径等。

奇安信安全DNS（QDNS）

奇安信安全DNS（简称QDNS），是由奇安信威胁情报中心与奇安信研究院联合推出的一款面向政府、企业与个人提供的DNS解析、威胁监测防御、资产/域名监控等一体的SaaS化解决方案，致力于为政企机构提供高速迅捷、纯净安全的全生态链网站安全防护体系。

04 本地威胁情报分析和运营系统

威胁情报平台（TIP）

帮助企业在安全运营中，利用威胁情报快速检测、响应、分析和预防各类网络攻击威胁，并分析产生行业威胁情报。

威胁情报运营系统（TIOS）

威胁情报运营系统（TIOS）是专为用户打造的一套完整的解决方案，基于本地环境的各类基础数据（文件、网络流量、各类日志）解决本地化威胁情报生产、分析、运营、服务中心的建设需求。

05 TI INSIDE-威胁情报内生产品解决方案

TI Inside 计划

TI Inside计划通过威胁检测引擎集成方式让网络安全威胁情报生态联盟（CEATI）内部合作伙伴的产品在短时间内即可具备基于威胁情报的检测能力，共同推动产品、解决方案层面的情报深度集成，共同推动威胁情报行业发展，为所保护的客户带来安全价值。

优势特色 ADVANTAGES AND CHARACTERISTICS

- 多源高级样本同源分析能力
- 恶意代码检测能力
- APT组织检测引擎RAS
- 威胁情报平台TIP
- 超强数据服务能力
- 完善的产品支撑体系
- 支持内生情报建设