安恒信息
DAS-security 安全中国

定制化威胁情报服务白皮书

文档版本：V1.5

发布日期：2021-10-11

www.dbappsecurity.com.cn

目　　录

1. 概述 2
1.1 基本概念 2
1.2 定制化威胁情报服务的意义 2
2. 服务实施标准和原则 2
3. 安恒信息定制化威胁情报服务 3
3.1 服务范围 3
3.2 服务内容 3
3.3 服务方式 4
3.4 服务流程 4
3.5 服务报告 5
4. 服务优势/服务特点 6
5. 客户收益 7
6. 为什么选择安恒信息 8
6.1 完善的威胁预警服务体系 8
6.2 专业的威胁情报支撑体系 8

1. 概述

1.1 基本概念

定制化威胁情报服务是由安恒信息安全研究团队为企业级客户提供的一项专业安全服务。安恒信息站在客户视角，为客户提供热点安全事件、安全漏洞、黑灰产活动的专业跟踪分析，并在第一时间向客户发送安全预警通告，致力于帮助客户在事前做好相关安全风险的收敛，减少安全事故的发生。

1.2 定制化威胁情报服务的意义

安恒信息通过整合公司的研究、产品、服务等能力，针对突发性威胁制定可落地的安全防护方案，旨在威胁事件爆发之前协助客户及时部署相关防护措施，保护用户的数据资产，提升企业应对威胁的能力。

2. 服务实施标准和原则

安恒信息定制化威胁情报服务遵守下列原则:

- 权威性原则：安恒信息定制化威胁情报服务中涉及的各厂商产品、设备的安全漏洞通告，均来自官方信息，其分析及解决方案由官方提供，对于尚未给出解决方案的漏洞，由安恒信息专家团队给出临时性 解决建议，确保信息权威、准确。
- 及时性原则：安恒信息提供的定制化威胁情报服务第一时间将信息通过 AICSO 平台、电子邮件等方式发给客户，保障客户能够第一时间了解、掌握最新安全风险。
- 实用性原则：安恒信息提供的定制化威胁情报服务以实用为第一要素，以防范安全风险为直接目的，安全通告中解决方案或建议，均经过专家团队的论证和实践，可信度，实用性更高。

3. 安恒信息定制化威胁情报服务

3.1 服务范围

安恒信息定制化威胁情报服务为客户提供权威、及时、准确的安全风险预警，第一时间将相关风险知会客户，并提供专业的解决建议。情报服务覆盖以下场景

- 漏洞场景：覆盖覆盖 CPU 处理器、网络设备、操作系统、虚拟化、容器、数据库、开发语言、中间件、应用组件等上百款软硬件产品的官方安全公告。
- 安全事件：覆盖国内外重要的 APT 攻击事件。
- 黑灰产场景：覆盖暗网、黑灰产社区的相关黑灰产情报。

3.2 服务内容

安恒信息定制化威胁情报服务以服务包的方式进行订阅。情报服务内容包括提供最新安全漏洞、威胁(0day、系统漏洞、网络攻击)、黑灰产情报、互联网侧的资产暴露面，以及相关问题的详情及解决办法或处置建议。情报服务包具体内容由以下可选模块组成:

- 安全漏洞订阅：对重要产品、软件、系统的安全漏洞安全更新进行实时跟踪，为客户提供漏洞简介、影响范围、安全建议
- APT 攻击事件订阅：对 APT 攻击事件进行分析，梳理攻击路径，提供排查方法和失陷指标
- 重点安全事件实时预警：对近期发生的重要安全事件进行分析（包括互联网侧近期关注的安全事件、APT 攻击事件、安恒应急响应中心应急中发现的攻击事件）,如 incaseformat 蠕虫病毒事件
- 暗网黑灰产活动实时监控：为客户实时监控来自暗网的黑产情报，定期知会客户

- 互联网资产暴露面监控：以攻击者视角和网络空间测绘视角为客户定期梳理在互联网侧的资产暴露情况，包括子域名、C 段、APP 资产、微信公众号等，提供详细的暴露资产清单

3.3 服务方式

- 通过 AiCSO 情报平台下发经安恒信息安全运营中心研判后的常规漏洞情报、APT 攻击事件/安全运营应急响应中心应急事件的失陷指标（包括恶意 IP、域名、URL、文件 HASH 等）供客户排查。
- 通过邮件订阅的方式第一时间为客户推送最新高危安全漏洞的预警通告，包括漏洞简介、影响范围、处置建议等。
- 定期输出定制化情报服务报告，包括互联网资产暴露面、黑灰产情报、安全漏洞回顾等。

3.4 服务流程

- 威胁监测：通过安恒信息应急响应中心、威胁情报中心、SUMAP、GreatMessage、暗网雷达等平台对主流软件、系统、设备的安全漏洞、和 APT 攻击事件、暗网黑灰产活动等情报进行实时监测。

- 威胁分析：经验丰富的安恒安全专家分析产生安全漏洞/事件的原因、受影响的范围、并给出相应的解决方法。
- 威胁研判：根据对威胁的分析，由安恒信息安全专家对相关情报进行研判，
- 威胁预警：针对常规漏洞类情报经专家研判后通过 AiCSO 平台下发，安全事件类情报由专家研判并提取 IOC 指标后通过 AiCSO 平台将相关失陷指标下发，重要安全漏洞经安恒信息专家研判后输出安全漏洞预警报告，客户的互联网资产暴露面、暗网黑灰产交易类情报经专家研判后定期通过定制化情报服务报告的方式同步至客户侧。
- 情报闭环：推动一线安服、驻厂工程师协助客户处置相关威胁，完成情报的闭环

3.5 服务报告

- 安恒信息安全研究团队严格按照安恒信息安全服务的流程，在服务期内，以严谨、认真、负责的态度对待每一位客户。对相关信息收集和分析后，形成《安恒信息定制化威胁情报服务报告》同时安恒信息按照客户要求为客户提供定制化威胁情报服务。
- 通过 AiCSO 平台推送安全漏洞情报、APT 攻击事件情报及 IOC 指标，一年内不少于 200 条。
- 《安恒信息定制化威胁情报服务报告》，按照客户实际需求定期为订阅客户推送。
- 《安恒信息高危漏洞预警》，相关漏洞爆发后第一时间推送客户，一年不少于 50 份。

4. 服务优势/服务特点

APT 攻击分析：猎影实验室提供了高级威胁研究及分析能力，对 APT 攻击事件进行深度分析。

0day/漏洞跟踪预警：GreatMeassage 平台提供实时安全漏洞监控追踪，覆盖覆盖 CPU 处理器、网络设备、操作系统、虚拟化、容器、数据库、开发语言、中间件、组件等上百款软硬件产品。安恒应急响应中心、分子实验室提供专业化的高级漏洞研究能力，为客户提供完整的漏洞解决方案。

暗网黑产实时监控：暗网雷达平台对暗网进行实时监控。

互联网资产暴露面监控：佩恩平台提供 7*24 小时监测服务，对客户暴露在互联网侧的资产进行检测和监测。

应急响应情报：安恒信息具有专业的应急响应团队，处理的应急事件遍布全国，覆盖全国 34 个省市 的多个行业，通过事件分析提取情报关键指标通过 AICSO 平台下发进行威胁狩猎。

5. 客户收益

掌握最新威胁动态：威胁爆发具有不可预期性，情报服务可以第一时间为客户提供威胁预警，识别风险，协助客户在事前做好加固与防护，减少安全事故的发生。

高危漏洞预警：安恒信息 AICSO、佩恩平台可根据客户信息资产情况为客户提供较为精准的安全预警通告，让客户第一时间知会期受影响的资产清单，快速、精准预警并响应，将风险控制于爆发之前，降低因安全事件导致的损失。

感知互联网暴露风险：依托安和信息佩恩平台强大的数据能力，为客户实时感知在互联网侧暴露的资产清单（包括，网站、APP、微信公众号等）。

挖掘打击黑灰产活动：安和信息暗网雷达平台为客户提供实时的暗网黑灰产活监控。

6. 为什么选择安恒信息

6.1 完善的威胁预警服务体系

安恒信息威胁预警体系是以公司安全运营中心为依托而建立，通过打通一线服务中心和二线安全研究能力中心的信息共享、能力传递实现了一套完整的威胁预警中台能力，从而可以对外提供专业化、定制化的威胁情报预警能力。

6.2 专业的威胁情报支撑体系

安恒信息威胁情报预警通告服务，拥有覆盖全国的庞大安全研究团队，包括安恒研究员猎影实验室、卫兵实验室、分子实验室、安恒风暴中心，具备强大的威胁情报数据平台，包括佩恩平台、GreatMesage 平台、SUMAP 平台、暗网情报雷达，可覆盖全场景下的威胁情报发现。