2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

内生安全 从安全框架开始

ENDOGENOUS SECURITY: STARTING FROM A CYBERSECURITY FRAMEWORK

此处放分论坛KV

威胁情报生态联盟介绍

Cybersecurity Ecology Alliance of Threat Intelligence

汪列军

观点

2015年

威胁情报引入国内

概念炒作期

2018年

威胁情报银弹论

辅量追捧期

2020年

情报默认INSIDE时代

落地优化时期

展，**下面摘录了《2020 SANS Cyber Threat Intelligence (CTI) Survey》的核心观点：**

1. **合作是关键**

尽管拥有专门的威胁情报团队的组织越来越多，但我们发现：**无论是通过付费服务提供商的关系或是通过信息共享组织或项目来使用威胁情报，均强调与彼此间的合作。**此外，组织内的协作也在增加，许多受访者报告说，他们的CTI团队是整个组织协调工作的一部分。

2. **并非所有处理威胁情报的过程都需要相同的自动化水平**

当涉及到数据处理时，半自动化可能是黄金标准，即使是一些经常被认为是冗余的任务，例如数据去重；因为在某些时候，数据去重中的部分信息是对分析人员是有用的。

3. **必要的数据和工具一直在随着CTI团队的发展而变化**

随着越来越多的组织开始产生他们自己的情报，CTI分析师需要的信息本质也从最初的威胁订阅或供应商提供的情报转变为来自内部工具和团队的数据。虽然可以使用许多类似的工具和流程来处理这类信息，但组织也必须明确如何使用合适的工具来处理内部生产的数据。

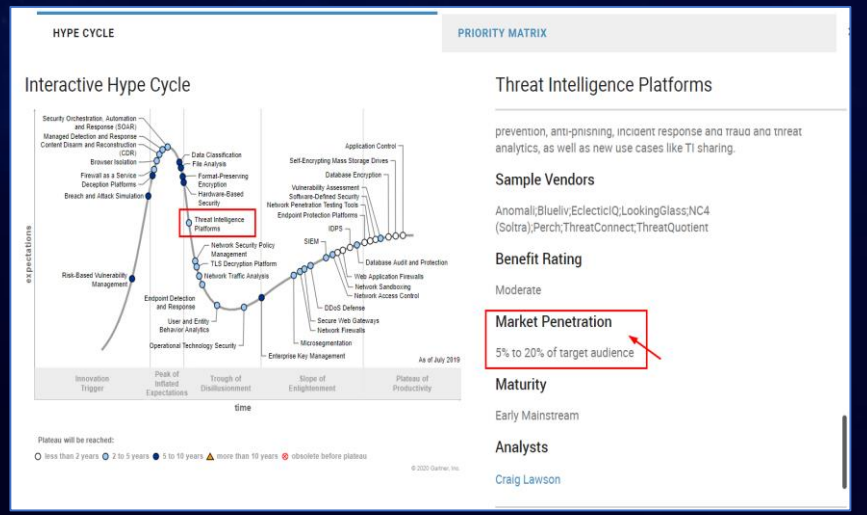
4. **成熟团队逐步形成对CTI的具体计划和需求**

需求是情报处理过程中的关键部分，有助于确保分析人员重点关注的情报收集和分析，以及适当的情报生产。这使得情报处理更有效率、更可测量——这是长期成功的关键。去年报告中，少数组织表示他们已明确定义和记录了情报需求；而今年，近一半的受访者表示他们已经定义并记录了情报要求。这是数据上的一次奇妙飞跃，鼓励人们在CTI项目中文档化记录对威胁情报的具体需求。

5. **消费和生产情报的共同体才能为CTI做出贡献**

SANS本以为在调研中会有更多的组织消费情报而非生产情报，但是实际调研发现：**超过40%的受访者既能生产又能消费情报——这是网空威胁情报领域日益成熟和专业化的重要标志。**只消耗情报或缺少任何优先的情报需求而难以满足组织机构中的大部分情报需求，他们因此考虑同时去生产和使用情报。

《Cyber Threat Intelligence (CTI) Survey》，2020，SANS



《Hype Cycle for Threat-Facing Technologies》2019，Gartner

威胁情报共享需要解决的问题

- 如何降低用户威胁情报消费门槛?
- 如何让更多用户更加便捷的使用威胁情报?

- 没有大数据怎么玩情报?
- 没有安全分析师又该怎么玩情报?

为了更好的威胁情报行业生态发展和威胁情报技术应用

我们联合国内多家著名安全厂商发起了威胁情报生态联盟CEATI

CEATI联盟有什么不同？

TI Inside计划：从最直接最见效果的基于IOC类威胁情报的检测能力输出做起，把检测逻辑和数据封装成SDK，联盟成员只要简单的引用集成就能完成能力的引入

情报能力的分享为纽带

SDK能力的集成为手段

联盟能力贡献成员：奇安信、天际友盟

联盟核心共享成员：各个集成SDK能力的厂商

CEATI联盟当前能力集成方案

能力描述	入门普通版	商业增强版	
能力提供方	奇安信	奇安信	天际友盟
定位	联盟内部成员免费	商业合作伙伴	商业合作伙伴
集成SDK	√	√	√
签署授权协议	√	√	√
请求入参对象	IP、域名、URL	IP、域名、URL	IP、域名、URL
情报类型	出站：失陷主机检测	出站：失陷主机检测 入站：实时黑IP	网关设备类IOC、流量检测设备类IOC、SIEM平台类IOC、
情报量级	5万/SDK	100万/SDK	全量实时明文数据包下载/STIXII
更新频率	小时级更新	小时级更新	小时级更新
分析研判支持	跳转CEATI联盟情报TI Portal分析平台	跳转CEATI联盟情报TI Portal分析平台（更多专业功能）	RedQueen在线查询平台

联盟成员权益

奇智威胁情报峰会

中国最悠久，最专业，最具影响力的威胁情报年度盛会，已成功举办3届，每年吸引近千人参会。前瞻性的主题、丰富的展区，专业的议程为中国威胁情报行业提供最硬核的交流平台。

- 联盟成员优先获得"奇智威胁情报峰会"的展位。
- 联盟成员可优先提交峰会演讲议题（演讲人，议题需经审核峰会委员会审核）。

审定的联盟成员可参加峰会晚宴。

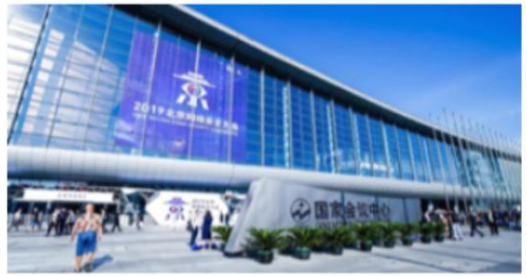
安全创客汇 Innovation Sandbox

中国最专业和悠久的网络安全创投平台，聚集了众多网络安全领域优秀的明星初创企业，自2016年启动以来，通过创客沙龙、年度明星赛、创业培训等一系列各类主题活动及服务，参赛企业赛后累计总融资额超过12亿元。

- 凡符合大赛要求的联盟企业可以直接进入线下半决赛环节。
- 联盟企业优先获得十大网安创投基金交流及直接投资机会，基金资金池过百亿。
- 联盟企业优先获得天津、南京产业园相关优惠政策（场地、税收、人才）

BCS北京网络安全大会 BCS BEIJING CYBER SECURITY CONFERENCE

中国规模最大、影响力辐射全球的国际化网络安全交流盛会，已成功举办7届，每年吸引近五万人参会，是网络安全界的达沃斯硬核安全大会。



- 参与威胁情报生态联盟展团，为威胁情报生态联盟成员在BCS大会提供展览便利。
- 为联盟成员贤良提供BCS大会期间产品发布，演讲议题等参会及活动权益
- 联盟成员在BCS会刊的优先传播权

联盟成员LOGO在大会印刷完，网页等传播素材露

CEATI联盟创始成员

CEATI联盟章程和组织架构详见官网

https://www.ceati.org.cn/

如何加入联盟？

加入联盟的企业需要在中国大陆地区具有：

✓独立法人

✓独立自主知识产权安全产品

✓产品覆盖有自有企业客户渠道

需要提供的基本信息

企业名称（全称）

企业营业执照

相关联系人

联系邮箱（企业邮箱）

联系电话

公司地址（省市县门牌号）

产品名称

产品软著

必要条件：须接受联盟提供的某种能力的集成

CEATI联盟成立仪式