C3安全峰会
CYBER | CLOUD | COMMUNICATION

威胁情报正在和企业安全架构全面融合

赵毅
谷安天下高级经理
安全牛高级分析师

C3

威胁情报正在和企业安全架构全面融合

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 一、概述 - 《威胁情报技术和市场指南报告》
- 二、应用场景及主要价值
- 三、案例：通过威胁情报分析行业风险
- 四、市场现状
- 五、局限性、挑战和趋势
- 六、资源

Summary
概　　述

《威胁情报技术指南报告》介绍

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 近年来，“威胁情报”一词迅速出现在信息安全领域，许多安全企业都在向客户提供“威胁情报”服务。但对于威胁情报一直以来并未有标准行业定义，以致于“威胁情报所到底指何物？我们如何利用威胁情报更好地完成工作？我们如何参考并建立威胁情报体系？”之类的问题，十分常见。
- 本报告对这些问题一一进行了分析和解答。文中描述了威胁情报的基本要素，介绍了威胁情报的技术实现原理，探讨了如何完成威胁情报的收集，分析、交付、使用工作，使得在不同场景不同层面上，协助包括基础作业层、专业技术层和管理决策层用户等人员更好地完成安全工作，并此基础上结合整体防御体系在探讨了威胁情报的未来发展趋势。
- 本报告由安全牛顾问团队，通过调查国内在威胁情报相关技术产品上作的较为突出的公司，并结合当前最新的相关资料撰写。

关键发现

- **1. 威胁情报是根据企业不同业务特征和需求，提供有关信息安全威胁，漏洞，事件和其他安全相关问题的信息。**同时提供关于攻击者的身份、动机、特征和方法的信息。而这些特性可以——从本文介绍的威胁情报需求，收集，分析、交付、使用的生命周期中得以体现，同时也让我们更加了解到底什么是威胁情报它又是怎样发挥作用的。
- **2. 威胁情报可以为不同层面的用户提供价值。**不仅仅为运维团队、安全应急团队等提供技术参考，还有一个非常重要的价值是协助用户决策层如何分配好合适的安全预算，评估企业第三方供应商的安全级别，来降低企业所面临的风险。
- **3. 威胁情报的技术应用需融入从威胁检测到应急响应的整个生命周期，全面减少安全风险暴露的时间，**而这个时间窗口是由企业防护者最为关心的、也是衡量企业安全能力的两条重要指标共同构成的，即**平均威胁检测时间**和**平均威胁响应时间**。
- **4. 行业标准及规范是建设威胁情报体系最好的参考，**STIX、 CybOX 、TAXII、OpenIOC、NIST 800-150、OpenDXL等都是威胁情报行业最具参考意义的标准规范。
- **5. 威胁情报在未来有望推动安全产品及服务模式的升级，使未来服务及产品的模式从“事件驱动安全”转向围绕“情报线索来驱动安全”的思路来进行。**同时，为催化新一代安全产品的产生起到指导性作用。

威胁情报的三个关键特征

Gartner定义：

“威胁情报是一种基于证据的知识，包括上下文、机制、指标、影响、操作建议等等，用来发现资产已经存在的问题或可能面临的威胁。”

- 我们从甲方的角度进行下解释：
- 威胁情报是以数据形式存在，由第三方专业机构提供的网络安全威胁信息，可进行传输交换、关联分析、挖掘应用，可以反映出组织存在的网络威胁和安全影响，不限于设备日志、报警或描述威胁事件的情报消息。并具备以下三个关键特征：**自身相关性、威胁源描述、多层面**

技术实现

安全需求：
数字资产、实体资产、无形资产、威胁源、威胁类型、风险偏好、角色、职责、使用场景

情报收集：
自动化和非自动化的手段，主动和被动方式，类型：IOC、Hash、黑名单等；情报源：开源情报、商业情报等

情报分析：
信息与情报、正确性与优先级；噪声-数据-信息-情报-可执行情报。

情报交付：
情报共享、可机读格式和自动化接口、可搜索知识库、针对性交付

情报交付：
基础作业层、专业技术层、战略决策层

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Application Scenarios and Value

应用场景和主要价值

基于用户角色的不同场景和价值

C3安全峰会
CYBER | CLOUD | COMMUNICATION

核心价值

对企业自身来说威胁情报作用于威胁检测到应急响应的生命周期，**缩短了检测和响应的时间**；

对于监管部门和风险控制部门来说提供了对监管对象和供应商**网络安全状况评价的客观依据**。

FIGURE 6 External Threat Intelligence Vendors And Capabilities (Cont.)

FORRESTER®

Finished intelligence
Raw intelligence
Tactical indicators

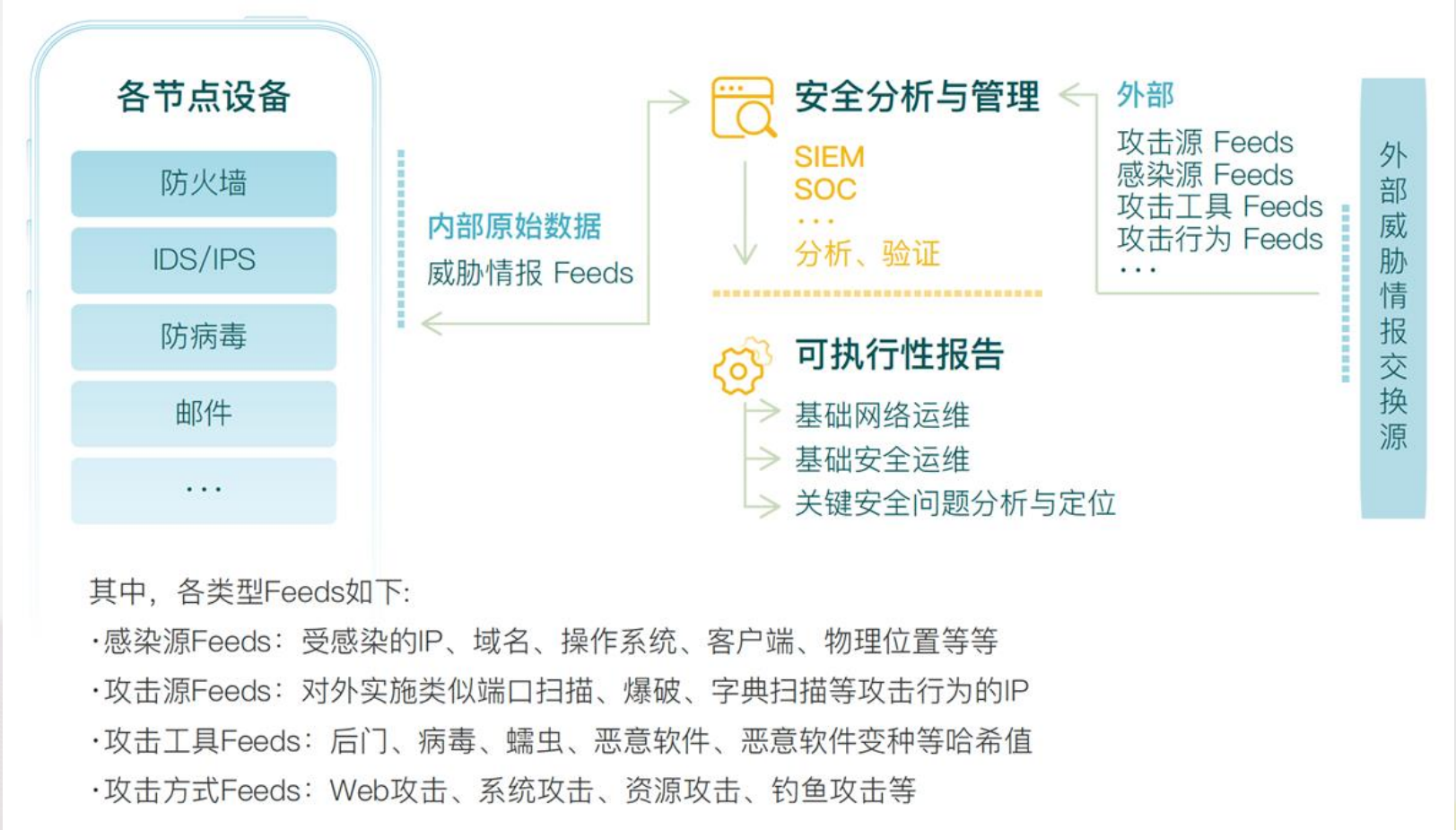
Vendor	Focus	Executive protection	Fraud intelligence	Brand protection	Vulnerability risk	Threat actor data	Insider threat monitoring	Third-party risk	Strategic intelligence	RFI
Proofpoint	Analyst expertise, global sensor network			●						●
PwC	Strategic focus on global and targeted threats				●				●	●

表 不同用户对威胁情报的使用

	基础作业层	专业技术层	战略决策层
角 色	基础运维人员 基础安全运维人员 安全服务人员	安全专家 应急小组 安全研究员	CIO CSO 信息化主管

为日常安全运维提供技术支撑

日常安全运维是基础设施安全保障的重要环节，参与该层面的人员包括**日常运维人员、安全运维人员、基础的安全服务人员**等；组织信息中心的日常安全运维人员在事前、事中、事后的安全事件处理过程中，利用威胁情报所提供的恶意软件签名、黑名单等数据对事件进行辅助判断，决定防火墙、网关、IDS / IPS系统和其他安全产品是否采取阻断控制。



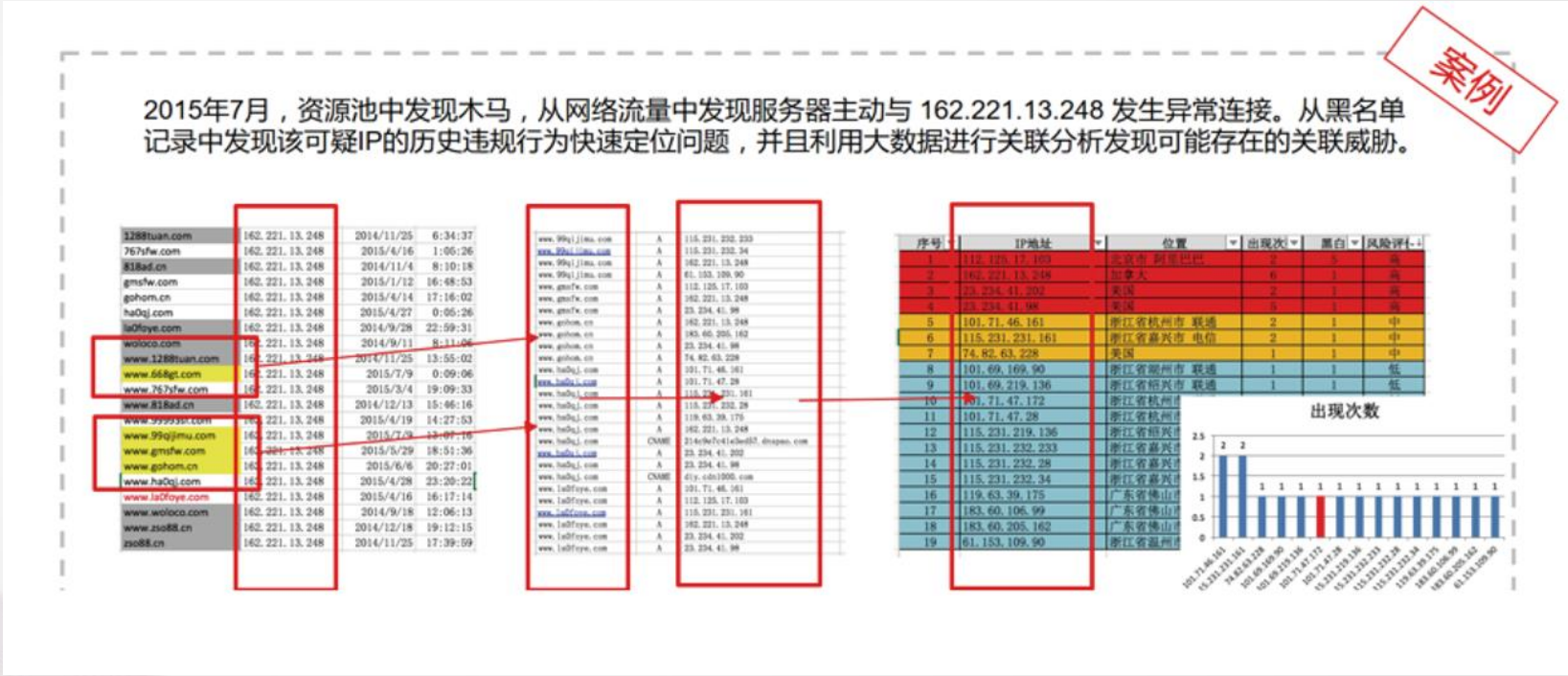
其中，各类型Feeds如下:

- 感染源Feeds：受感染的IP、域名、操作系统、客户端、物理位置等等
- 攻击源Feeds：对外实施类似端口扫描、爆破、字典扫描等攻击行为的IP
- 攻击工具Feeds：后门、病毒、蠕虫、恶意软件、恶意软件变种等哈希值
- 攻击方式Feeds：Web攻击、系统攻击、资源攻击、钓鱼攻击等

为专业安全分析提供有利资源

在情报领域常被提起“战术情报”，主要指导了专业的执行层面所需要的资源，网络安全对专业技术分析的要求比较高，很多服务商需要提高专业的服务能力，威胁情报在该层面发挥了重要的作用。

网络安全专家需要有关攻击者和攻击行为的深入情报，诸如恶意软件的分析，攻击目标的漏洞成因，以及对手的战术、技术和程序（TTP）的报告等



为风险决策管理提供客观依据

威胁情报帮助管理层，包括组织的CIO、行业主管部门领导对下级子公司或者分支机构进行管理，实现全方位快速的了解行业内的安全状况，并对安全预算，流程改进，新技术和人员配置水平做出更好的决策。组织自身对第三方（供应商、合作伙伴）的安全管理需求也是迫切的。一份有价值的评估报告能帮助他们最大限度地降低风险，从而保障业务和计划的健康发展。

例如：Gartner在2016年报告中出现了一种新概念——安全评级服务(SRS, Security Rating Services)

	机构数	安全漏洞	络攻击	圾邮件	尸网络	意代码	黑名单
银行	100	26%	35%	22%	32%	27%	4%
券商	100	31%	30%	14%	14%	22%	3%
基金	100	18%	13%	5%	10%	4%	3%
保险	100	28%	24%	11%	12%	5%	5%
第三方支付	100	24%	67%	6%	37%	2%	2%
小贷P2P	100	12%	55%	1%	27%	5%	3%
投融资（众筹）	100	4%	28%	1%	20%	0%	7%
企业征信	100	11%	27%	0%	14%	0%	3%
互联网保险理财	100	16%	45%	1%	19%	1%	4%
金融综合服务	100	15%	39%	1%	25%	2%	2%

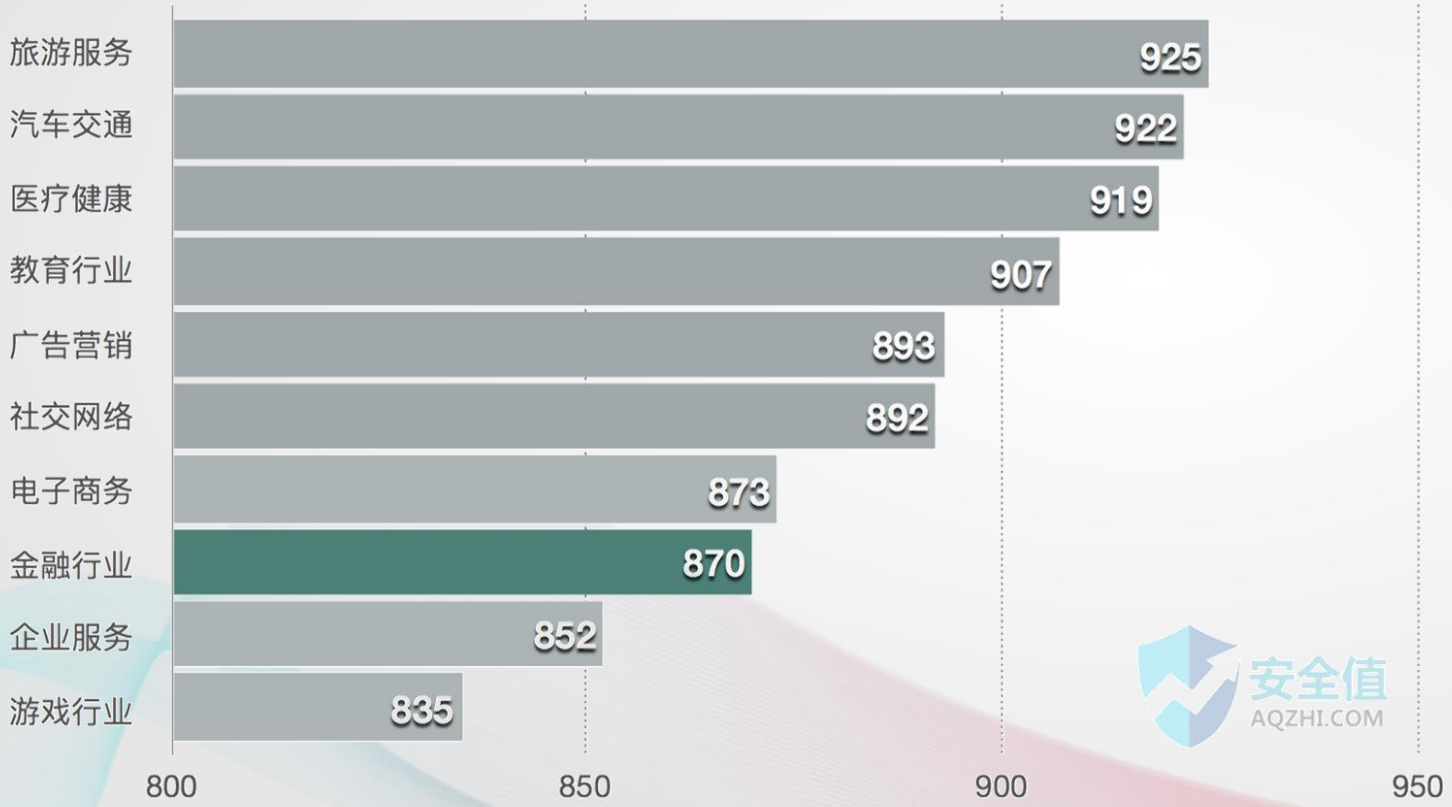
以上数据来自《10大金融领域2017年6月网络安全报告》

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Case：Industry Risk Analysis By Threat Intelligence

案例：通过威胁情报分析行业风险

从外部视角评价各行业安全状况



分析对象选择：

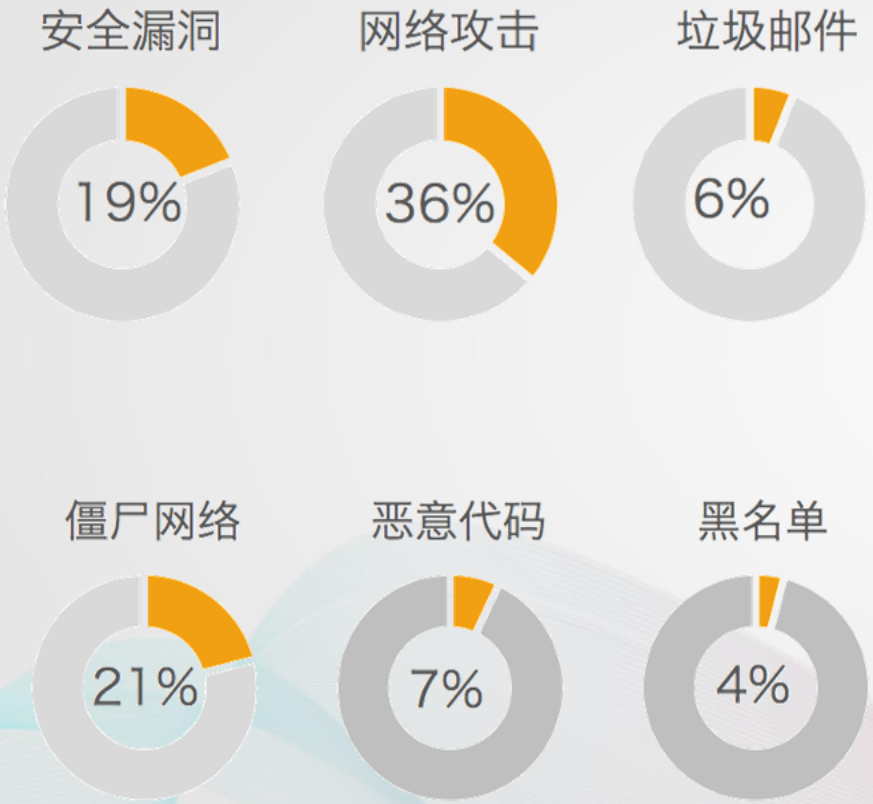
基于20个行业6万家机构数据中选择网络安全关注度较高、较流行的10个行业10000家企业/机构。

分析数据：来自外部100多个安全数据资源，自2017年1月至6月的安全事件数据。

报告数据来源：

安全值*《金融行业10大领域2017年6月网络安全报告》*

金融行业10大领域外部安全威胁分析



	机构数	安全漏洞	络攻击	圾邮件	尸网络	意代码	黑名单
银行	100	26%	35%	22%	32%	27%	4%
券商	100	31%	30%	14%	14%	22%	3%
基金	100	18%	13%	5%	10%	4%	3%
保险	100	28%	24%	11%	12%	5%	5%
第三方支付	100	24%	67%	6%	37%	2%	2%
小贷P2P	100	12%	55%	1%	27%	5%	3%
投融资（众筹）	100	4%	28%	1%	20%	0%	7%
企业征信	100	11%	27%	0%	14%	0%	3%
互联网保险理财	100	16%	45%	1%	19%	1%	4%
金融综合服务	100	15%	39%	1%	25%	2%	2%

关键问题分析：安全漏洞

CVE编号	漏洞名称	数量	漏洞说明
CVE-2015-0204	OpenSSL FREAK Attack漏洞	314	该漏洞是由于OpenSSL库里的s3_clnt.c文件中，ssl3_get_key_exchange函数，允许客户端使用一个弱RSA秘钥，向SSL服务端发起RSA-to-EXPORT_RSA的降级攻击，以此进行暴力破解，得到服务端秘钥。此问题存在于OpenSSL版本0.9.8zd之前，或1.0.0p之前的1.0.0，或1.0.1k之前的1.0.1；http://cve.scap.org.cn/CVE-2015-0204.html
CVE-2014-0160	OpenSSL Heartbleed 心脏滴血	40	（OpenSSL Heartbleed 心脏滴血）在OpenSSL1.0.1版本的心跳包模块存在严重漏洞（CVE-2014-0160）。攻击者可以通过构造特殊的数据包，直接远程读取存在漏洞的OpenSSL服务器内存中多达64KB的数据，极有可能导致网站用户帐号密码等敏感数据被非法获取。漏洞发现者甚至声称可以直接获取到证书私钥和重要的商业文档；http://cve.scap.org.cn/CVE-2014-0160.html
CVE-2016-9244	Ticketbleed	10	（Ticketbleed）是F5 BIG-IP设备的TLS / SSL堆栈中的软件漏洞，允许远程攻击者一次提取高达31字节的未初始化内存；http://cve.scap.org.cn/CVE-2016-9244.html
CVE-2017-7269	IIS 6 远程代码执行漏洞	8	开启WebDAV服务的IIS 6.0被爆存在缓存区溢出漏洞导致远程代码执行，目前针对 Windows Server 2003 R2 可以稳定利用，该漏洞最早在2016年7,8月份开始在野外被利用。http://cve.scap.org.cn/CVE-2017-7269.html
CVE-2015-2080	Jetty web server远程共享缓冲区泄漏漏洞	2	如果你运行着存在漏洞的jetty版本，那么你的密码，请求头，cookie，anti-csrf令牌，token等等一系列的东西遭到黑客窃取。比如post请求中包含的信息。http://cve.scap.org.cn/CVE-2015-2080.html

领域	评估机构数量	漏洞机构占比	漏洞数量
银行机构	100	26%	50
证券公司	100	31%	46
基金公司	100	18%	28
保险公司	100	28%	46
第三方支付	100	24%	98
小贷P2P	100	12%	16
众筹&投融资	100	4%	4
企业征信	100	11%	15
互联网保险理财	100	16%	31
金融综合服务	100	15%	40
总体	**1,000**	**19%**	**374**

关键问题分析：网络攻击

- 常受到拒绝服务攻击的端口 80、4444、443、53

领域	评估机构数量	被攻击机构占比	攻击事件数量
银行机构	100	35%	713
证券公司	100	30%	263
基金公司	100	13%	1,331
保险公司	100	24%	2,058
第三方支付	100	67%	12,967
小贷P2P	100	55%	18,852
众筹&投融资	100	28%	7,503
企业征信	100	27%	3,049
互联网保险理财	100	45%	6,359
金融综合服务	100	39%	34,877
总体	**1,000**	**36%**	**87,972**

威胁地址	事件数	地址信息
221.238.7.97	6048	天津市
180.213.7.20	4717	天津市
117.25.222.122	3943	福建省厦门市
124.200.96.218	1948	北京市
221.238.191.122	1677	天津市
27.191.225.23	1326	河北省唐山市
219.141.149.59	969	北京市
65.48.174.139	922	巴巴多斯
62.212.236.10	876	阿塞拜疆
1.193.145.232	762	河南省洛阳市

Top 10 威胁金融行业的恶意地址

Market Situation
市场现状

市场分析关键发现

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 情报数据驱动安全市场，很多客户希望能够引进和了解新技术，建立“大数据安全分析平台”或“态势感知平台”项目，必然会引用威胁情报技术作为支撑，并**将内、外数据进行关联分析，实现全面感知网络威胁。**
- 目前国内“威胁情报”还属于发展初期，独立的采购需求并不高，从提供商角度统计市场空间每年仅有数千万（不包括传统产品和服务升级而扩大的市场）。但是，**它不是孤立存在，目前更多的是做为基础能力，落地到厂商的典型产品和服务中**；
- **当前国内威胁情报应用主要集中在IT成熟度比较高和安全要求较高的行业**，如：金融（至少股份行以上）、政府（监管为主）、能源和特大型企业，总体客户规模数十个，其它行业的应用较少；另外只有一些行业中比较领先的企业和机构正在应用，其它企业无论从驱动力和自身能力方面都持关注的态度。
- 规模较小、专业性较强的威胁情报厂商在短期内还是**需要大量资本投入**的，从人员能力要求到存储计算资源的投入都是一个比较高的预算；另一方面拥有完善销售渠道和丰富产品线的大型厂商也会加大投入，组建几十人的专业团队和大量资源来支撑威胁情报做为基础的新产品，以巩固已有的产品市场份额，提高技术门槛。
- 技术交付形态包括：**产品、工具、数据、报告**

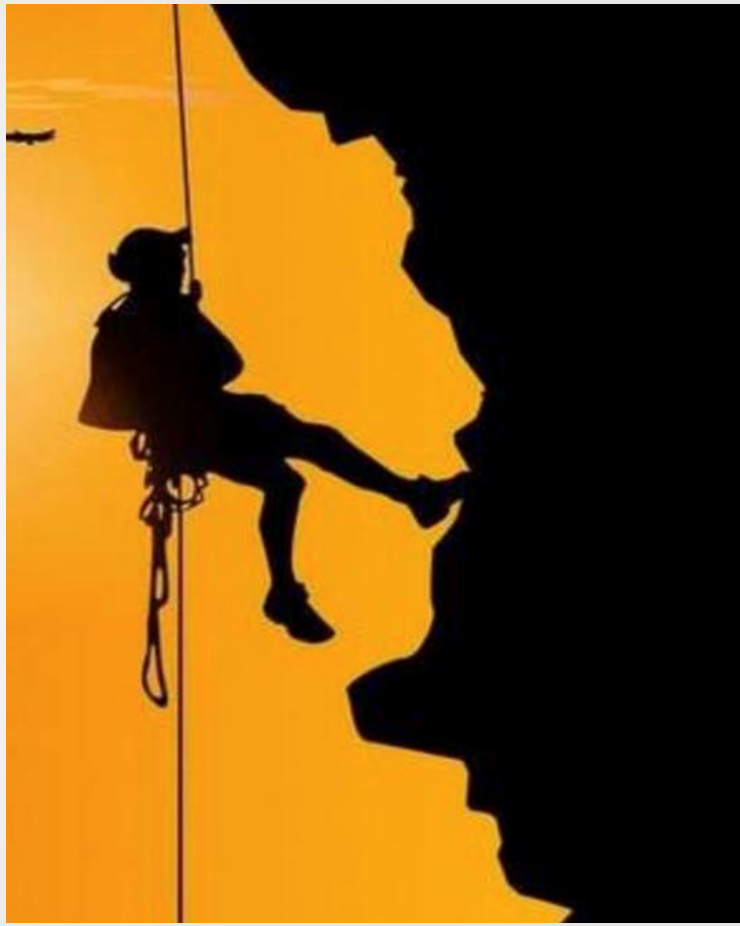
C3安全峰会
CYBER | CLOUD | COMMUNICATION

Limitations, Challenges and Trends

局限性、挑战和趋势

局限性和挑战

- 数据价值的挖掘和分析需要一定基础，门槛较高
- 不同行业和业务场景下的需求差异较大，缺乏针对性的应用方案和产品
- 行业协同能力与机制尚未成熟，导致服务水平不一致



未来趋势

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 与传统产品和服务结合，形成新一代产品
- 在细分领域上出现新产品及服务形态
- 形成中国特色的或行业规范的的威胁情报标准
- 相关产业链中将形成不同体量的合作群体
- 基于用户需求推动多种类的情报发展

Resources
相关资源

相关资源

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 相关标准： STIX、 CybOX 、TAXII、OpenIOC、NIST 800-150、OpenDXL
- 威胁情报数据资源： OTX、 X-Force Exchange、 VirusTotal、 MUTE、CTX、 Spamhaus …
- 开源威胁情报工具： SpiderFoot、 OSTrICa …
- 感谢参与本次调研的相关厂商：360企业安全、微步在线、天际友盟、白帽汇、数字观星、默安科技

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You