为实现
成功的网络威胁情报交换
构建坚实基础

期望在云环境
安全事件响应方面进行协作的
公司需考虑的关键问题

cloud security alliance®

目录

鸣谢 **4**

序言 **5**

概览 **6**

寻找适合你的评估共享计划 **9**

建立共享关系 **10**

评估交换平台的能力 **10**

建立信任 11

参与者匿名保护以及数据清除（Data Sanitization） 11

开放标准 12

自动化 13

规模化分析 13

协作 14

行业/同业组织小团体（enclaves） 14

时间同步 14

在你加入之前为成功构建基石 **15**

捕获内部事件威胁 **15**

考虑如何使用情报观点 **15**

衡量是否参与和价值 **16**

制定策略 **16**

入门威胁情报交换操作指南 **17**

威胁情报交换框架 **18**

识别可疑事件 18

收集相关事件数据 19

决策如何去共享数据以及与何人共享 20

事件反馈与关联的监控器 **23**

评估合作响应的需要 **23**

下一步号召行动 **24**

附录 A共享事件信息示例 **25**

附录 B额外资源 **26**

鸣谢

网络事件共享工作组联席主席

Dave Cullinane Brian Kelly

主要贡献者

Ramsés Gallego

Krishna Narayanaswamy Edgar Odenwalder

Rich Phillips

贡献者

Mariano J. Benito Ryan Bergsma Olivier Caleff Elvis Hover

Leo Magallan Christine Mullaney David Neuman Kavya Pearlman Codina Ramon Carlos Samaniego

Stacy Simpson

Jeff Valdes John Yeoh Richard Zhao

中文版翻译说明：

由中国云安全联盟(C-CSA)秘书处组织翻译为实现成功的网络威胁情报交换，构建坚实基础 Building a Foundation for Successful Cyber Threat Intelligence Exchange，中国云安全联盟专家委员会专家翻译并审校。

翻译审校工作专家：（按字母顺序排列）

组长：沈勇。组员：冯春进 、方伟 、胡泽柱 、李建民 、罗义兵 、马红杰 、马韶华 、魏琳琳 、张威。

C-CSA工作人员：

赵元勋（C-CSA 研究助理）

翻译术语

Data Sanitation：数据清除

Data Redaction：数据修订

Enclaves：小团体

CIE：网络事件交换

threat vector：威胁向量

序言

当前网络攻击的频率和复杂程度在不断提高。攻击者可能是个人，也可能是资源丰富、组织严密的团伙。面对这样的威胁，企业如果只关注内部防护措施，可能建成最后被绕过“马其顿防线”；如果只依赖自身的情报能力，可能面临攻防不对等的窘境。为了解决上述问题，网络威胁情报（CTI, Cyber Threat Intelligence）及其交换计划成为近年来安全建设的一个热点。企业在建设自身情报能力，选择和加入合适的共享计划方面需要具体、专业的指导。在美国国土安全部（DHS）、美国国家与技术研究所（NIST）、恶意代码信息共享平台（MISP）、欧洲网络与信息安全局（ENISA）的早期研究成果的基础上，云安全联盟（CSA）不仅推出云计算网络事件共享中心（CloudCISC, Cloud Cyber Incident Sharing Center）为联盟会员提供最先进的威胁情报交换计划；而且发布了本文，为那些希望利用威胁情报加强自身安全能力的企业提供指导。文中还特别指出了云提供商（CSP）在威胁情报领域的独特地位。中国云安全与新兴技术安全创新联盟（简称：中国云安全联盟）组织业界专家翻译为中文版本，相信一定会有助于更多的中国企业从威胁情报中获益。

中国云安全联盟和云安全联盟大中华区非常感谢翻译和支持工作者们和中国云安全联盟专家委员会专家们的无私贡献。

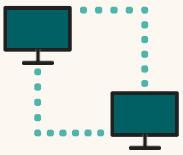
中国云安全与新兴技术安全创新联盟常务副理事长
CSA云安全联盟大中华区主席
李雨航 Yale Li

概览

没有组织可免受网络攻击。恶意攻击者结合了技巧和敏捷性，快速有效地在目标间移动。新的攻击在一开始的24小时内，只针对几十家公司，几天内就扩散到几百家公司。[1]几年前，对威胁环境具备可见性已经是关键能力，如果希望网络安全具备一定预防能力。今天，了解即将发生的事情对于维持（系统）生存至关重要。

复杂的组织，特别是云提供商，是否能区分小事件和大规模入侵依赖于它们快速检测，控制和减轻攻击的能力。提升事件响应速度已经成为云提供商的重中之重，他们正越来越多地参与到行业内各种网络事件信息交换的计划中。（此类计划）有时称为威胁情报交换或网络事件交换，这些计划使云提供商能够与可能遇到相同问题或面临相同类型攻击风险的其他人共享网络事件信息。

不可否认，网络安全信息共享在过去对安全团队的价值有限。虽然这部分是由于过去在自由交换网络威胁数据方面的法律和文化障碍，但主要挑战是因为以前的信息分享计划是手动和响应式的。这些计划更侧重于在威胁被检查，清理和缓解之后，再分享有关网络安全事件的信息。这更像是一种公开服务而不是一个支持快速事件响应的工具。虽然这些数据有明确的目的，也曾发挥一定作用，随着攻击速度和数量的增长，他们的价值降低了，另外，此类信息共享在少数关键技术设施部门之外未得到广泛采用。



不仅云提供商对网络威胁情报交换感兴趣，安全高管以及各行各业的思想领袖们也正对其进行重新审视。在美国，网络威胁信息共享被纳入美国国家标准与技术研究院（NIST）的一个自愿框架中，该框架旨在降低网络基础设施面临的风险，既是风险评估，也是事件响应活动，并将其作为一个支持和促进网络风险管理的手段，在《关于加强联邦网络和关键基础设施网络安全的风险管理》的美国总统行政命令中强调。.

NIST网络安全框架

美国总统行政命令《关于加强联邦网络和关键基础设施网络安全的风险管理》

1 2017 Data Breach Investigations Report 10th Edition by Verizon, April 27, 2017

概览（续）

快速切换到今天的安全环境和网络事件信息交换，透过以前的信息共享计划，几乎无法辨认。 随着安全运营中心（SOC）和计算机安全事件响应小组（CSIRT）的成熟，威胁情报、数据分析和安全事件管理方面的新技术和工具为更快速、可执行的威胁情报交换创造了新的条件。

事件数据 -- 更准确地说可疑事件数据 -- 现在可以跨团队、跨工具、甚至跨公司进行快速地进行分享和分析，成为即时响应流程的一部分。事实上，如果一个组织等到他们发生“事件”以后才开始共享信息，那太迟了。现在重点是在识别可疑事件的第一时间共享相关数据，这大大加快了补救工作，并为尚未受影响的组织提供了早期、可执行的警告。

这种新型威胁情报交换模式的积极影响在2017年5月的Wannacry危机期间得到了证明。尽管第一个感染报告起源于5月12日在西班牙，但英国和苏格兰遭受这个恶意代码的打击更为严重。这在很大程度上归功于西班牙政府对关键基础设施的事件响应方案，例如来自全国密码学中心2的警告，该警告迅速确定了恶意软件及其传播媒介、提供了缓解工具，并鼓励各组织共享这些信息。西班牙公司能够迅速保护自己免受Wannacry的攻击，然而这个恶意代码在其他国家继续蔓延。 英国国家网络安全中心（NCSC）3传播的威胁情报，提供了理解和关于分享最佳缓解措施的指导，为Wannacry病毒提供最终的关闭开关。

云提供商在威胁情报交换中扮演着独特的角色，因为他们不仅拥有和管理着世界上大量的IT基础设施，而且还运营着一些在科技领域最领先的计算机安全事件响应小组/安全运营中心（CSIRT/SOC） 。由于这一投资，他们可以说是处于最佳位置来运营共享情报以防护他们的系统。此外，由于他们能在很大的规模上做到这一点、并能包含行业中很大的一部分，他们有切实的机会帮助（行业）与恶意攻击者保持在同一起跑线上对抗。 CSA也在推动一些行动来帮助其会员实现这两个目标。

1 https://uk.reuters.com/article/us-spain-cyber/telefonica-other-spanish-firms-hit-in-ransomware-attack-idUKKBN1881TJ

2 https://www.ncsc.gov.uk/blog-post/finding-kill-switch-stop-spread-ransomware-0

概览(续)

作为一系列文件的第一篇，本文提供了一套框架，来帮助那些正在寻求加入威胁情报交换计划以加强自身事件数据分析和事件响应能力的企业。本文的目标读者是那些对网络安全数据交换刚开始考察、或已经开始交换的企业。旨在为安全团队提供帮助，无论其内部威胁情报能力是刚建立的还是已经成熟。事实上，只要有专职的威胁情报人员，组织就需要考虑加入威胁情报交换计划来强化自身的数据。为此，本文将在3个关键领域为企业提供宏观的实践指导支持:

- 与最能满足其需求的共享合作伙伴和交换平台进行连接
- 识别能力和业务要求，它们是价值驱动的威胁情报交换计划的基础
- 理解交换过程的基本原理，以便他们可以有效地共享其所见的事件数据并更有效地操作他们收集的任何情报

本文中的指南由云安全联盟（CSA）网络事件共享工作组[4]的成员开发。此成果已用于Cloud-CISC（云网络事件共享中心）的设计、开发和运营，Cloud-CISC[5]是为CSA成员提供威胁情报交换的平台。这些建议主要基于通过**Cloud-CISC**[5]的开发和运营获得的经验教训，以及管理大型公司威胁情报计划的个人经验。这项工作一些常见的挑战包括：

1. 对其内部事件数据难以理解的组织很难决定其应该共享什么事件数据。
2. 虽然他人提供了威胁情报，但通过电子邮件形式传送会导致不能很好地集成到事件响应流程中，所以价值通常很有限。
3. 组织希望能够横向扩展到其他部门并在供应链中纵向扩展。
4. 共享的动机不是一定要帮助到其他方，而是为内部响应能力提供更好的支持。

本文旨在直接解决这些挑战，并为那些开始进行威胁情报交换的企业建立一个关键考量的基本框架。我们希望与行业内的其他机构合作，进一步开发此指南并制定相关的最佳实践，使威胁情报交换成为面临日益严重威胁的所有组织的宝贵资源和社区。

4 CSA Cyber Incident Sharing Working Group **https://cloudsecurityalliance.org/group/cloudcisc/#_overview**
5 CloudCISC **https://www.csa-cloudcisc.org/**

寻找适合你的评估共享计划

精心设计的共享计划可以为成员提供大量支持，并使不同成熟度级别的组织能够参与并从外部威胁情报交换中获取价值。虽然旧有的信息共享计划仍然存在并且尚有一席之地，但今天的重点应该放在威胁情报交换的新模式上，它不仅仅是在威胁结束后实现共享。更确切地说，网络事件交换应该实现三个关键目标：

1. **启用共享。** 在响应过程中安全，方便，及早地分享有意义的网络事件数据，以便在补救工作中利用外部数据并提供早期预警以帮助其他人降低风险暴露。
2. **拓展专业技能。**与来自经过审查的云提供商/云客户的熟练安全分析师协作，分析攻击指标，制定防御策略并缩短缓解时间。.
3. **提供背景和支持决策。**避免重复劳动，从其他方的经验教训中获得收益.

旧有信息共享计划	威胁情报交换计划
在事件经过检验、分析甚至经常在缓解后，才分享事件信息	一旦识别可疑事件数据立即分享
数据共享经常通过邮件自动分发系统或者手工	数据以多种形式共享，包括API
经常依赖于可靠第三方数据手动擦除机密信息或者提交的个人信息	利用加密和其他技术提供自动化、匿名性以及敏感或专有数据的修订（redaction）

本章将回顾交换平台和共享计划（例如但不限于CloudCISC）的作用以及这些如何帮助支持参与者。就本文而言，交换平台被定义为支持事件信息交换的基础系统，并允许公司与业内同行、政府和其他相关外部组织形成共享关系。

建立共享关系

公司有许多机会与外部组织发展共享关系。虽然有一些威胁情报平台协助公司促进其与同行的直接共享关系，但许多新进入威胁情报交流领域的组织一开始是加入相关行业团体，特别是本行业中的信息共享与分析中心（ISAC）、信息共享和分析组织（ISAO）、特定行业的计算机安全事件响应小组（CSIRTs）/计算机应急响应小组（CERT）。ISAC/ISAO/CSIRT/SERT这类组织在促进特定行业的网络安全信息方面有着悠久的历史，其中很多已经实现了基础设施现代化，使其上运行的威胁情报交换平台可以提供强大的、自动化的数据分析能力。依据其需要，公司还可以选择与国土安全部（DHS，Department of Homeland Security）的自动指标共享（AIS,Automated Indicator Sharing）服务[6]进行共享（这是一个DHS支持的，主要由私营企业和公共部门合作伙伴共享威胁情报的生态圈），或与特定行业CSIRT提供的恶意软件信息共享计划（MISP） 服务进行的情报共享.

评估交换平台的能力

CSA 认为，云计算在全球IT基础架构中独树一帜，几乎无处不在，因此云计算行业有权领导威胁情报分享。面向云提供商的共享计划（Cloud-CISC），2015年成为试点项目，并在一年后推出公开测试版。其目标是开发威胁情报交换计划，充分利用威胁情报和“大数据”分析方面的最新成果，具体地、无缝地支持成员的事件响应工作流。

CSA很荣幸能为会员提供最先进的威胁情报交换计划。

CloudCISC设计为向成员提供实时的事件共享和分析，使得CSA成员的事件响应工作立见成效。

事件报告一旦共享后，CloudCISC平台的独特算法就可以将其与其他合格成员所提供的报告进行几乎实时的关联。若发现相似之处，会向成员发出警报并提供相关的报告，包括其他攻击指标、有价值的情境信息和处置建议。成员还可以决定其他的合作方式，例如加入响应工作。

所有CSA的公司会员都可以在限定时间内免费注册两个CloudCISC许可证。 我们鼓励公司会员今天在https://www.csa-cloudcisc.org/注册。

6 Department of Homeland Security’s Automated Indicator Sharing (AIS) service https://www.us-cert.gov/ais

首先，是否参与特定共享计划的决定应由组织的自身业务和安全需求驱动。此外，成熟的组织不应将其威胁情报共享局限在一个团队或系统，而应通过与多个共享组织发展伙伴关系来挖掘价值。而且，在共享计划的设计和能力、及支持它们的交换平台是如何直接影响用户的参与率和他们的辛勤努力所换来的价值等方面，已经汲取了许多经验教训。描述Cloud-CISC的运营能力对于实现所述的威胁情报共享目标至关重要，这将有助于公司评估共享计划和交换平台。

建立信任

为了实现共享，应该在计划运营方及参与者间建立起一定程度的信任。这可通过标准的保密协议（NDA）或协议备忘录来实现，约定提供者和所有参与者可以在威胁情报交换成员内部共享。此外，计划运营方应审查所有未来的成员，以确保他们是以合法目的成为交换平台成员的合法组织。

有时交换计划会细分出几个由成员领导牵头的小组织，也被称为小团体（enclaves），交换平台运营方将向成员提供一份标准的保密协议（NDA）和和审查支持，推动这些较小团体的协作。

应确保未来的参与者们理解信息交换平台是否提供参与贡献数据的激励措施，以及不参与共享的后果。 基于激励的参与方式鼓励所有成员积极共享，使得信息交换平台和各参与方都能获益 。

参与者匿名保护以及数据清除（Data Sanitization）

从传统信息共享工作中吸取的一个重要教训是，公司必须有一种方法来确保无意中泄露的机密事件数据不会破坏他们的品牌、客户信任和核心业务。这个方法就是通过在威胁情报交换中成员匿名和数据清除（Data Sanitization）实现的。

值得注意的是，与CloudCISC的经验强调了通过交换平台匿名提供信息的好处。通过确保被共享的事件数据不能回溯其来源，企业共享信息所面临的风险大大降低。 这使得CloudCISC成员可以在应急响应流程中更早地分享更丰富的数据，从而快速启动协作响应工作。

参与者应该有能力通过对他们的提交信息匿名化来保护他们的身份。威胁情报交换平台应该知道提交者是被授权的成员，也许能够获得关于提交者的有限的地理位置信息（比如区域），但是它不需要知道更多的信息。交换平台的供应商和其他交换者不能够确定哪些公司提交了哪些数据。

虽然提交者知道哪些数据应该被混淆来以确保提交是匿名的，但是不同的交换平台对参与者提供了不同级别的支持、自动化处理和保护。一个推荐的方式就是通过哈希混淆。该方法允许不同的提交者之间的数据相互关联时而不用说明其特定身份。如果有四家公司提交相同的散列值，这些数据可以相互关联并且可帮助这四家公司更好地应对可能发生的情况。

输入到威胁情报交换平台的信息应该被清除任何相关的公司数据。虽然报告实体有责任执行这一行动，但不同的交换平台将为参与者提供不同程度的支持，并可能提供不同的输入格式。至关重要的是，参与者要理解数据清除（Data Sanitization）是如何实现的，这样他们才能确保所有机密的公司信息都得到保护。

最后，一些交换平台提供了一种“预览”功能，允许公司输入他们自己的数据，并在向更多的受众者公开前查看存在相关性的信息。

开放标准

在一次交换过程中，参与者越多，它能收集的事件数据也越多，同时其成员间的关联利益也越多。理想情况下，交换平台不应采用商业上受限的技术或单一输入格式来限制参与者。例如，虽然结构化的威胁信息表达（简称STIX）[7]和自动交换（简称TAXII）的可靠的指标信息被迅速接受作为信息共享规范，但许多公司并没有实现它们，尤其是小型企业。支持广泛参与的能力对于希望使用威胁情报交换的公司来说尤其重要，因为交换可以理解供应链内的风险和事件。

因此，交换平台应该使用开放协议和非商业限制的基础设施。这意味着有能力接受任何格式的数据。在评估一个有更多限制性的平台时，参与者应该了解其局限性，并确保它能够顺利地集成到这个有更多限制性的环境中。.

7 在国际范围和免费的公共使用情况下，TAXII和STIX是以社区驱动的技术规范设计的，能够为网络安全态势感知、实时网络防御和复杂的威胁进行自动配对信息共享。更多的信息： **https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity**

自动化

事件响应小组很忙，所以易用性必须是一个考虑因素。对分析师来说，输入数据的工作必须迅速而简单，确保提交的数据已经剔除掉公司特定的机密信息。威胁情报交换平台应该提供自动化工具以支持方便快捷的数据提交。

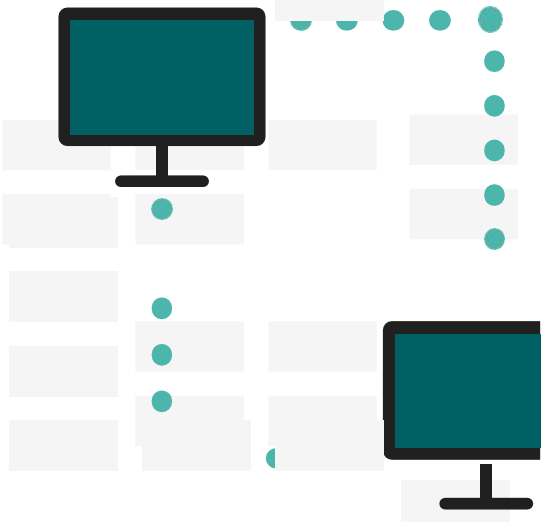
此外，与安全事件管理（SIEM）系统集成的能力是必不可少的。SIEM应该能够利用来自威胁情报交换平台的应用程序编程接口（API）。其他自动化功能包括电子邮件接收和通知，可以帮助事件响应人员在发生事件时更迅速地通知并与对等组织协作。

规模化分析

响应时间必须是分钟级的，而不是小时或天级别的。当一个事件响应团队识别出潜在的攻击时，他们有很多的事情要做，而留给他们做决策的时间相对较少。提交给一个威胁情报交换平台的可疑事件必须迅速而准确地关联起来，并且必须以一种易于分析师检查和操作的格式快速返回。

为了实现这一点，一个威胁情报交换平台必须能够有效地执行大规模的分析。理解一个交换平台是如何关联和管理"大数据"的，是评估它在事故发生时能提供何种实时帮助的关键。

由网络事件交换（CIE，Cyber Incident Exchange）返回的信息应该是可操作的和上下文相关的。数据可视化功能可以极大地帮助参与者快速查看事件数据与他们组织及其环境的关系。理想情况下，交换平台应该有能力显示各参与成员共享的数据中的相关联的信息。例如，一个实体提供的信息应当在威胁情报交换中随时通知相关实体，一旦其信息包含在相关的事件操作中心（IOC，Incident Operation Center）中。



协作

接收对新威胁的预警是有益的。但是，当威胁情报交换允许团队在管理已识别和潜在的威胁时与他人实时协作，那么它即构成事件响应过程战略的一部分。如果社区中的某个人已经找到了修复方案，那么应该迅速散播出去，这样进行情报交换的任何成员都不必重新造轮子。这种协作可以让组织利用他人的专业知识来捕获威胁，并在发生攻击时缓解攻击。这对中小型公司尤其有利，他们有时候很难聘用和留住威胁情报领域的顶尖人才。交换计划通过其选择的平台，可提供一些特别的工具，主要包括：匿名或署名聊天/消息的能力；共享SIEM脚本或其他可能有助于共同社区的方法;与在相同源头中事件数据传播的成员共享或附加的备注； 对于每日、每周或每月的交换活动的标准摘要报告。

行业/同业组织小团体（enclaves）

可控、安全和经过批准的分组允许行业同行成员彼此分享信息并在向更广泛的受众发布数据之前解决问题。分组内的组织往往通过保密协议（NDA）获得批准。在本文中，我们将这些小组称为小团体（enclaves）。包含小团体（enclaves）将允许一个拥有共同利益的较小团体参与单独的交换，以在彼此之间共享数据。 例如，在向航空业以外的更大受众发布与给定威胁有关的信息和数据之前，航空公司的独立团体可以解决彼此问题。在独立团体内共享的信息仍然是专有的，直到该小组决定将其发布给更广泛的相关组织的交流社区。

时间同步

时间同步对于故障排除至关重要，对于事件关联更为重要。威胁情报交换中的所有设备和对等点应通过通用的NTP分层解决方案进行同步，该解决方案将由标准的NTP Stratum[8]提供。

8 如需了解更多关于NTP Stratum的信息，请参见：www.ntp.org.

在你加入之前为成功构建基石

鉴于威胁情报交换的先进能力，特别是在自动化和协作领域，成功参与网络事件分享并不需要限于具有高度成熟的情报和响应能力的组织。 任何公司，哪怕只有一人致力于威胁情报，都应该考虑参与情报共享计划，以增强自己的数据。

威胁情报交换可以成为威胁情报管理和事件响应功能的宝贵资产。我们越来越多地看到这两种功能集中于SOC。在SOC中，分析人员管理多种工具，产品和工作流程，包括SIEM，工单和编排平台，威胁数据来源，漏洞扫描和端点检测产品。

无论公司具备一名还是三十名分析师，为SOC添加另一种工具的想法可能令人望而生畏。但如果使用得当，威胁情报可以成为加速并简化调查工作的有力工具，从而为安全团队节省宝贵的时间。为实现这一目标，组织应采取一些措施来帮助确保将威胁情报交换成功整合到其SOC工作流程中。

捕获内部事件威胁

许多安全分析师在加入威胁情报交换之前，都会监控大量的工具、存储系统和数据输入。许多供应商通过SOC监控容器、混合架构和深入的供应链。组织应该创建并维护一个从自己系统中捕获的公共的事件数据存储库。通过观察存储库中报告的事件，关联到自己组织中的相关事件，公司将更好地了解来自威胁情报交换的新数据如何影响它们。执行内部分析使它们能够快速确定如何和何时与外部交换共享事件数据。通过这种方式，情报共享完善了他们现有的威胁情报行动，而不是仅仅增加另一个新的监控。

考虑如何使用情报观点

加入威胁情报交换计划将丰富组织的事件数据，但前提是要考虑如何使用这些数据。公司发现他们经常无法轻易整合来自专有威胁提供商或共享中心的外部威胁反馈。有时候，这是由于外部威胁情报交换中的事件报告和相关性不佳造成的，但也可能是安全分析师缺乏规划和支持的结果。通过手工筛选包含可疑IP地址列表的电子邮件不仅费时，其价值值得怀疑，更有可能累垮公司精英。

为了避免这些问题，组织应该制定一个他们如何将从交换计划中获得的威胁情报运用于操作的计划。他们整合威胁情报交换的计划应该确定情报可以用于告警，分类，调查和缓解内部事件的方式。这包括自动化关键流程并选择一种工具来帮助分析师实时关联数据，并更轻松地提取关键指标。自动化和工具还应仔细考虑选定的威胁情报交换平台如何向组织传输数据。

衡量是否参与和价值

任何新的时间和资源的投资，都应该根据其回馈给安全运营的价值，进行持续评审。组织应定义他们通过参与情报交换可以达成的期望和目标，并考虑将如何衡量投资的回报。通常的目标是 ，SIEM调优、获取更好或更多的相关行业的运行情报，以及获得更多有关具体威胁向量（Threat Vector）的战术情报。

组织目标应包括安全团队围绕共享的活动的明确目标和操作数据，获取和提供关于如何分享支持缓解过程数据的反馈，以及一些从接收较早的攻击指标从而导致网络风险降低的考虑。

制定策略

在与参与网络事件交换（CIE，Cyber Incident Exchange）相关的考虑确定之后，将它们记录在事件交换政策中是有用的，这次政策将置于更广泛的事件响应计划和组织整体安全策略之中。这些文件化的政策可能包括：

- 使用目的
- 角色和职责（例如，可能包括谁被授权输入数据，谁被授权看到结果，谁被授权对数据进行研究等）
- 与数据安全性有关的交换的提供者的要求
- 数据输入要求
- 保留数据的要求
- 事件中的责任

入门威胁情报交换操作指南.

本节中的指导旨在帮助企业更好地理解威胁情报工作流程，以便他们能够更有效地将其集成到他们现有的安全运营中。我们的目标是帮助企业在交换平台上有效分享信息，并更有效地摄取和操作他们收到的威胁情报。

这是一些工作组在制定本指南时使用到的交换事件和威胁信息的指导原则。基于几个垂直行业、风险偏好、技术和运营成熟度等几个特征，虽然业务和技术要求因不同组织而异，工作组发现Cloud-CISC成员之间有几个共同的重要期望。这些期望推动了威胁情报交换模式及相关的最佳实践的发展。具体包括:

- 没有上下文的安全（或事件）信息是不完整的。上下文对制定明智的运营和商业决策是必要的.
- 信息分类必须为其服务和/或消化的方式提供敏捷性，以支持及时的决定和行动。
- 数据越多越好，可以更好地分析基于证据的信息和风险评估。
- 不要对法律、政策和风险限制做出假设，并邀请主题专家进行分享。

本白皮书为威胁情报交换过程提供了一个模型，并包含CloudCISC成员迄今为止发现的一些最佳实践概要。

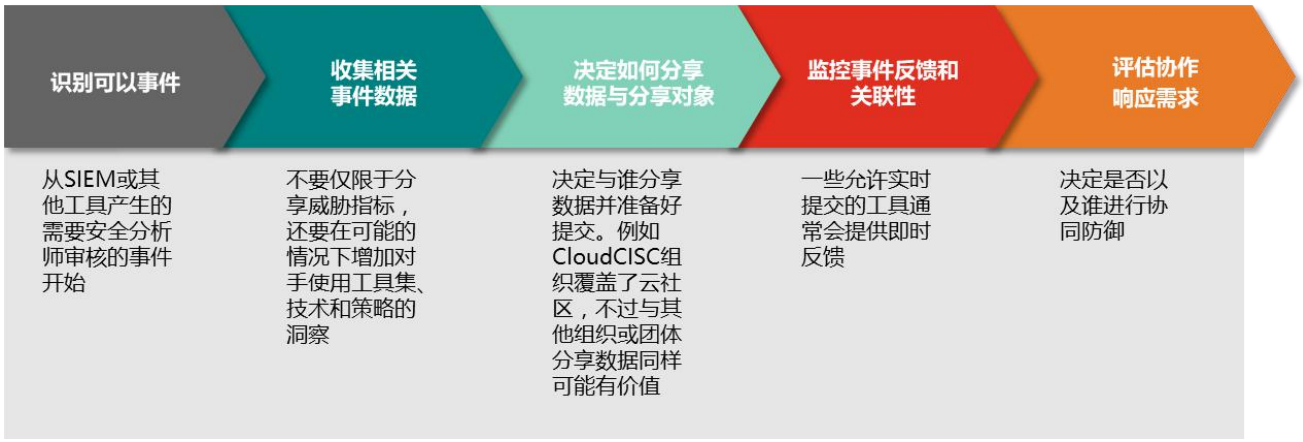
然而，我们的目标是以更详细的实践指导，继续支持企业每一阶段的交换过程。

这个努力由CSA的CloudCISC工作组领导。我们积极寻找反馈和志愿者来帮助推动这个领域内未来的指导。如您对为此贡献感兴趣，请访问

https://cloudsecurityalliance.org/group/cloudcisc/#_join

威胁情报交换框架

虽然自动化驱动了许多威胁情报的过程，但是人类在评估和理解数据方面的作用不可低估。安全分析师的职责是决定什么是重要的以及如何行动。自动化程序为他们提供了他们所需要的数据；但是最后的决策过程是由他们进行的。本框架特别侧重于标识在威胁情报交换流程中进行决策的关键点。因此，关注点不在于可能有所不同的，组织用来消费和生成信息的方法（技术平台，工具使用等等），而在于如何使用信息进行决策和采取行动来保护这些守护者需要守护的环境和数据。



识别可疑事件

网络事件情报交换的基础始于理解内部收集的信息，以便能更好地了解已识别事件的潜在可能性和影响。考虑到被监控事件的数量巨大，对响应活动进行优先级排序的能力是至关重要的。

确定优先级的开端可以从SIEM为安全团队审查所提供的数据或一个触发问题管理系统的事件开始。

下一步则是根据组织对其信息技术生态系统的相对了解来确定事件潜在可能性和影响。例如，了解什么样的IT资产（数据库，网络组件，认证信息等等）处理，存储或传输特定数据类型会对业务（财务，健康，个人信息等）造成影响。这些综合知识为安全团队确定合规程序以及根据潜在可能性和影响来确定优先级提供了基线。

一旦一个事件为审查确定了优先级后，安全团队随后可以准备与社区分享相关信息。

收集相关事件数据

从纯粹意义上来说，安全分析师试图发现对手的能力、意图以及针对定义的有价值资产可能采取的行动，从而让自己可以采取最好的行动来应对攻击。尽管信息共享通常集中在很有用的威胁指标上，但安全团队通常可以获得更丰富的数据来推动决策。这些丰富的数据包含对手使用的策略、技术和过程（TTP，Tactics, Techniques and Procedures）。根据观察低级别的指标变化很快。然而，对手的策略、技术和工具集（TTP）变化需要很长一段时间，部分原因是这需要他们花费很高的投入水平和资源来进行开发。

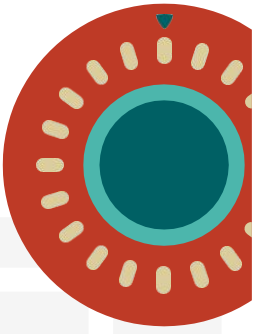
这可以使用鱼叉式网络钓鱼攻击的例子来说明。鱼叉式网络钓鱼的方法可以被认为是TTP，而电子邮件的内容则是潜在威胁指标。在这个例子里，钓鱼邮件的内容（即指标）很容易改变，并且对于防备较弱的目标可能仍然很容易成功，但是TTP却没有改变。

同时分享对手的TTP信息和指标信息是很有用的。但是，推动不同的活动，都需要不同的事件响应速度。

为了绕过防御措施指标会更频繁变化。指标需要迅速采取防御行动来识别，遏制和消除它们。在鱼叉式网络钓鱼的例子里，可以将指标加入反垃圾邮件平台，以便在发现威胁时立即缓解威胁。相比之下，TTP可以并且应该驱动更广泛、更长期的基础设施防御活动和措施。在鱼叉式网络钓鱼中，这些活动可能包含使用或配置反钓鱼平台，以便在对手获得访问权限前消除这些攻击路径。这种配置通常由基础设施团队实施并且可作为多年的有效防御。

除了指标和TTP之外，安全分析师通常可以访问有关事件的其他信息。可能包含的信息元素包括活动发现位置，哪些活动先于并且遵循该特定指标，主要针对哪些特定目标或目标团体，以及是否针对特定的垂直行业。这些信息元素允许对行为进行分类，从而帮助设计和构建防御措施。

一个经常被讨论但不太相关的信息是归因（attribution）。归因是困难和耗时的，并且从实际角度来看，对于响应过程而言，归因相对于识别能力，意图和可能的行动方式的行为来说作用不大。在大多数情况下，归因不需要在威胁情报交换的情况下处理。



总之，鉴于事件数据的丰富性已经超过威胁指标，目标应该是通过威胁情报交换尽可能多的情境信息。通过这样做，组织不仅可以为其他公司提供丰富的数据来推动决策制定，而且理想情况下他们还提供了更多的线索，可以帮助自身和其他人填补决策制定和响应过程中的数据空白。

情境化数据的价值可以通过Wannacry攻击相关事件来展示。当美国政府使用的漏洞被释放出来的消息披露后，跟踪并开始情境化威胁的团队可以在内部共享信息并向其组织提供明确的建议。结果，他们可以减少自身组织的攻击面，并且在方程式组织漏洞被勒索软件利用时以及对抗未来与Wannacry相关漏洞时都能做出更好准备。

附录 A 提供了一个通过网络事件交换（CIE，Cyber Incident Exchange）进行包含情境和基于证据决策事件信息分享的示例。

决策如何去共享数据以及与何人共享

当前有很多技术平台、技术形式和技术方法可以进行内部和外部的信息共享。对每个组织来说，可能选择信息共享的途径是唯一的，但在具体执行操作时也有一些额外的东西需要考虑。就像前面几节内容所讨论的，交换平台可以提供基于数据分享机制各方面的支持和自动化操作。但更进一步来说，如果在这个过程中存在围绕威胁情报交换而制定的制度化政策，则将简化应对个别事件的决策流程。下面则列出了主要的考虑事项。

授权访问和审批过程

共享信息的授权访问和审批流程应该在策略中被定义，而不是为每次事件评估这些决定，强烈推荐这种方式。此外，组织必须注意的是，威胁情报的交换在数据迅速共享时是最有价值的，可以获取到更多关于检测到的威胁的价值并提供预警给其他人。较长的审批流程则明显会对达成这样的目标起负面作用。根据我们的经验，只要确保了所有组织的身份和机密信息在信息共享的过程中没有安全风险，匿名和数据修订（Redaction）可以极大地加快这个过程。

社区共享

很多组织都参加到多个共享计划中。也有一些组织甚至参与到某个共享计划内的一个小组或小团体（Enclaves）中。对于每个事件，安全团队都需要决定事件信息的分享范围，是广泛地共享给他们参与的所有共享计划，还是只在其中的一两个计划，或甚至仅仅是小团体（Enclaves）。一般来说，最好的做法是尽可能广泛地分享可疑事件的信息。然而，在某些情况下，事件的敏感性可能会要求组织限制其分发。例如，组织可以决定某事件只能在支持匿名提交的威胁情报交换平台上共享。或者是限制其只能与行业成员进行共享，直到知道了更多关于这个事件的信息。

匿名提交

可疑事件及其周围的数据通常会包含来源组织的敏感信息。同时，在有效的情景化事件中可能需要该数据。这种匿名交换事件的方式可以很好地管理存在的风险。在某些情况下，交换平台本身就具备匿名性。对组织来说，准确地了解什么样的数据在交换过程中被泄漏是很重要的。通过确保共享的事件数据不会被溯源，（共享情报）企业的风险就算没有被完全消除，也会大大降低。.

机密和敏感数据

通常会存在这样一些与网络事件有关的信息，它是敏感信息、但与消费端采取行动却无关。这些敏感信息可能会包含顾客个人身份可识别信息（PII）或者知识产权。提交组织承担保护这些信息的最终责任是。因此，应该在提交给给威胁情报交换平台之前从事件中删除这些信息。有时可以通过交换平台的客户端支持自动完成这个修订（Redaction）过程。如果平台没有此功能的话，组织将需要一种管理数据修订（Redaction）的方法。在字段信息被特殊字符替换的时候，可以是非常直观的方式（例如，用Y替代X）。可以在整个字段或部分字段内容上进行修订（Redaction）。例如，“n”或“m”字符结尾可以保留在明文中，其余字符可以被修订（Redaction）。另一种用来避免无意泄露的技术是混淆一个字段的长度，它用固定的或随机数量的修订（Redaction）后的字符替换文本。

数据格式

用于信息交换的数据格式可以是二进制，也可以是冗长的自然语言构造。冗长类型的表示将更适合于网络事件信息交换。还应该注意的是，在一些SOC中正在建设高水平的自动化网络事件信息消费能力。有一些数据格式是冗长的，同时适合于机器消费。属于这一类的最常用的数据格式是XML和JSON。

多种类型的网络安全用例依赖于这样的网络事件信息，包括事件管理/日志记录、恶意软件表征、入侵检测/预防、事件响应和数字取证。一个标准化的语言支持着网络事件共享在广泛的应用范围被有效、无缝地消费。一种用于信息交换的标准化语言是结构化威胁信息表达式（STIX）[9]。

STIX框架旨在传达全范围的潜在网络威胁数据元素，力求表现力、灵活性、可扩展性、可自动化性和人类可读性。OASIS[10]开放标准组的下属的一个技术委员会正在积极在STIX上工作。STIX规范定义了不同类型的STIX域对象（SDO）。

STIX 域对象实例

Indicator Object


```
{
 “type”: “indicator”,
 “id”: “indicator--031778a4-057f-48e6-9db9-
 c8d72b81ccd5”,
 “created”: “2017-02-09T12:11:11.415000Z”,
 “modified”: “2017-02-09T12:11:11.415000Z”,
 “name”: “HTRAN Hop Point Accessor”, “pattern”: “[ipv4-
 addr:value = ‘223.166.0.0/15’]”, “labels”: [
 “malicious-activity”
 ],
 “valid_from”: “2015-05-15T09:00:00.000000Z”,
 “kill_chain_phases”: [
 {
 “kill_chain_name”: “mandiant-attack-lifecycle- model”,
 “phase_name”: “establish-foothold”
 }
 ]
}
```


STIX是一系列威胁情报规范的一部分，旨在帮助自动化和构建网络安全信息共享技术。其他规范包括可信的指示器信息自动交换（TAXII），它定义了一组服务和消息交换，以及网络可观察表达式（Cybox）。Cybox是一个标准化的模式，用于在所有系统和网络操作中观察到的事件或状态属性的规范、捕获、表征和通信。过去Cybox是作为一个独立的项目开发的，但现在已经集成到STIX 2.0项目中。

9 https://www.oasis-open.org/news/announcements/stix-v2-0-and-taxii-v2-0-are-now-oasis-committee-specifications

10 https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

STIX和TAXII是获得良好支持的威胁情报规范，推荐那些具有实施资源的组织使用它们。然而，威胁情报共享不应排除无法使用这些规范的组织。因此，最佳实践规定交换平台应该允许以任何格式包括电子邮件和文本的数据的吸纳和集成。

事件反馈与关联的监控器

任何共享可疑事件数据的组织应确保可以将事件相关信息返回给它们，并与原始事件数据相关联，以支持其响应和缓解（mitigation）努力。一些交换平台自动支持这个过程，但是组织应该确保他们准备好保持反馈循环打开，并且能将任何社区提供的事后解决方案数据用户操作。

评估合作响应的需要

缓解（mitigation）一些事件可能是直截了当的，但缓解另一些可能需要组织内不具备的专业知识或经验。此外，可能还有一些事件，某个组织可能希望贡献自己独特的洞察力，它有助于同行的缓解努力。安全分析师需要确定是否需要外部协作来解决一个事件以及如何启动这一努力。通常，交换平台将通过安全聊天等方式帮助建立协作小组。其他时候可能需要直接联系其他受影响的组织。

下一步号召行动

CSA 认为，任何使用威胁情报的公司都会从外部威胁情报数据交换中受益。公司不再被要求冒着他们的生于、资产或客户受损的风险来参与单向安全地分享网络安全信息，而只有很少的回报。现在是拥抱新方法的时候了。

因为云计算产业已经利用了许多支持威胁情报交换的先进技术，并且在IT基础设施上拥有如此独特和庞大的足迹，所以有一个真正的机会，使威胁情报共享无处不在。我们对该行业的承诺是继续为我们的成员提供价值驱动的威胁情报交换，并支持他们通过开发和发布相关指南和最佳实践来参与。虽然云社区是我们的首要任务，但我们相信，我们的努力将成为整个IT界寻求威胁情报交换价值的典范。

本文仅是一系列计划中的第一次努力，以提供指导、赋能使威胁情报交换的新用户使其从先行者的经验教训中收益。我们要求社会各界人士提供我们迄今为止的工作反馈，并通过分享最佳实践和经验教训，为我们的持续努力作出贡献。

最后，我们呼吁所有的企业CSA成员加入Cloud-CISC。我们的产业承受不起继续闭门造车了，而任由恶意分子和我们做对。现在是时候公平竞争，甚至可能获得优势了。

附录 A共享事件信息示例

影子经纪人（Shadow Brokers）最新泄露针对Windows OS和SWIFT银行系统

今天，影子经纪人，这个网络小组，因为自从2016夏季以来几次泄露了美国国家安全局（NSA）的黑客工具而闻名，发布了一个新的文件集合。这些文件包含了针对微软Windows操作系统（OS）的漏洞和黑客工具，以及一系列关于从几个全球银行的SWIFT银行系统收集数据的演示和文件。该组织利用其Twitter帐户抛出这些文件和密码，随后将其解压缩并上传到在GITHUB上，供大规模使用和安全研究员们分析。新的发布包含了三个文件夹，命名为“Windows”、“Swift”和“Oddjob”，其中包含23个新的黑客工具。

关键点

- 新的复杂黑客工具的源代码都可被研究人员和威胁实施者使用
- 这次抛出的文件时间可以追溯到2013年，但是，到今天，其中一些攻击方法仍然是有效的
- 对所有Windows版本的总体影响仍然是不清楚的
- 成为目标的几家使用SWIFT系统的银行很可能遭到入侵
- “Windows”文件夹包含多个Windows黑客工具和可执行文件。看起来与2016年12月公布的材料不同。“Odd job”文件夹包含一个名为ODDJOST的植入程序，并包含详细的配置文件和有效载荷信息。据称文件夹包含一个2013文本文件，突出显示ODDJOBIT成功绕过了一些由著名的反病毒提供商（如赛门铁克、卡巴斯基和F-Secure）提供的反病毒软件平台。 “SWIFT”文件夹包含一个演示文件和一些以JEEPFLEA MARKWT冠名的文件，讨论swift联盟访问（SAA，Swift Alliance Access）系统。此外，此文件夹包含SQL脚本，用于搜索SWIFT特定的数据、文本和微软 Excel文件；暗示者（此黑客工具）的操纵者进入了全球多家银行，主要是在中东国家。值得注意的是：许多攻击方法似乎是基于内存的，降低了传统的、非基于非行为的（入侵）指标的效力.

建议防御行动

- 防御行动1：在接下来的30天内，设立优先级，为公司使用的所有微软Windows版本安装补丁/更新
- 防御行动2 ：积极监控媒体和安全研究组关于威胁源采用（新的）攻击能力和未来目标的信息发布

参考

Medium, Vice, GitHub

附录 B额外资源

政府资源

国土安全部自动指示器共享（AIS）服务
https://www.us-cert.gov/ais

国家标准与技术研究所（NIST）网络安全框架
https://www.nist.gov/cyberframework

加强联邦网络和关键基础设施网络安全的总统行政令
https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

恶意代码信息共享平台（MISP，Malware Information Sharing Platform）
http://www.misp-project.org/features.html

欧洲网络与信息安全局（ENISA）
https://www.enisa.europa.eu/news/enisa-news/enisa-publishes-first-study-on-cyber- threat-intelligence-platforms

https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms

网络安全的信息共享规范

概述
https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

关于OASIS网络威胁情报
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

STIX 2.0 (包括CYBOX)
https://www.oasis-open.org/news/announcements/stix-v2-0-and-taxii-v2-0-are-now-oasis- committee-specifications

TAXII
https://www.oasis-open.org/news/announcements/stix-v2-0-and-taxii-v2-0-are-now-oasis- committee-specifications

