

2017 年 10 月 3 日, 星期二

Beers with Talos 第 14 期: 威胁排名和避免不专业的漏洞响应



Beers with Talos (BWT) 播客第 14 期现已上线。下载本期播客并订阅 Beers with Talos:



如果您对 iTunes 和 Google Play 不感兴趣, 不妨试试 Beers with Talos 播客:
www.talosintelligence.com/podcast

第 14 期亮点集锦:

我们有一段时间没有轮流介绍自己了 (在这段时间里我们又有了大约 5 万次下载), 所以这期我们会用平时每期开始前抱怨某些事的时间来做自我介绍。

在过去六个月左右的时间里, 我们遇到了大量“顶级”威胁。就像关公战秦琼一样 (其实就是), 节目组试着对近期的以下威胁/攻击进行了排名: CCleaner、Deloitte、Equifax、Nyetya、SEC、Shamoon2、WannaCry。不可思议的是, 我们每个人给出的排名竟然各不相同。您的排名又是什么样的呢?

关于响应: 一致性很重要, 切忌自作聪明。我们会讨论一下最近在安全响应方面看到的令人难以置信的一些蠢事。更重要的是, 我们会讨论应该如何应对安全事件。

请记住: 复杂性带来问题。但是它坑不了思想领袖。

第 14 期导听:

01:30 - 畅所欲言 - 你是谁?

12:35 - 威胁排名 - 2017 年是“供应链攻击年”吗?

37:50 - 漏洞响应: 好的、坏的、拙劣的 - 坦白地承认吧

53:10 - 复杂性坑死人

59:20 - 结论和零星想法

链接:

“如何成为思想领袖”视频: https://www.youtube.com/watch?v=_ZBKX-6Gz6A
Talos 博客“语言表达中的不确定”: <http://blog.talosintelligence.com/2017/08/on-conveying-doubt.html>

=====

节目组成员: Craig Williams (@Security_Craig)、Joel Esler (@JoelEsler)、Matt Olney (@kpyke) 和 Nigel Houghton (@EnglishLFC)。

主持人: Mitch Neff (@MitchNeff)

查看所有节目:

<http://cs.co/talospodcast>

通过 iTunes 订阅 (欢迎发表评论!)

<http://cs.co/talositunes>

查看 Talos 威胁研究博客:

<http://cs.co/talosresearch>

订阅威胁源新闻通讯:

<http://cs.co/talosupdate>

在 Twitter 上关注 Talos:

<http://cs.co/talostwitter>

对我们的主题提供反馈和建议:

beerswithtalos@cisco.com

发布者: MITCH NEFF; 发布时间: 20:38