

思科安全智能研究与分析团队 Talos



保护客户，防御已知和新出现的威胁

如今的企业用户，需要网络安全产品能够提供领先的威胁情报智能，从而有效地保护自己的网络。而提供领先的威胁情报智能是思科 Talos 安全情报与研究团队的核心关注点。

Talos 团队，由领先的威胁研究人员组成，通过对复杂的系统进行分析，为思科的安全产品提供全面的威胁情报智能，从而保护客户，防御已知和新出现的威胁。Talos 依靠思科最为完善的基础设施，对遥感数据进行收集、关联和分析，进而提供无以伦比的可见性，其中涵盖的系统包括：

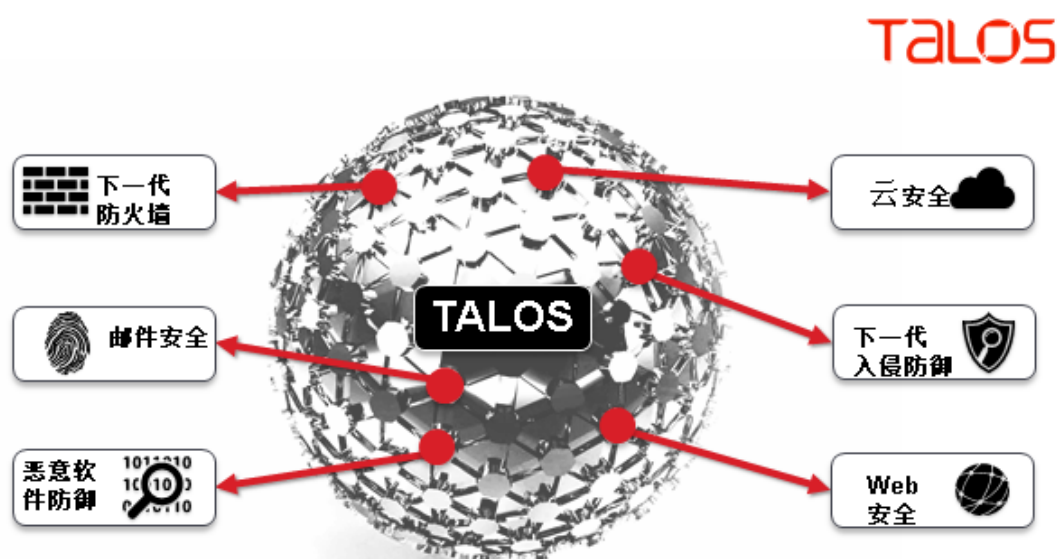
- ✓ 数以千亿计的 Web 请求和电子邮件
- ✓ 数以百万计的恶意软件样本
- ✓ 开源数据集
- ✓ 数以百万计的网络入侵

通过这些分析，我们可以得到的是一个安全的云智能生产大数据分析，这个分析涵盖了包括网络，终端，移动设备，虚拟系统，Web 和电子邮件威胁在内的众多平台。它也为客户提供了对威胁的更为全面的理解，包括威胁的根源，爆发的范围等，而将这些智能加入到用户侧网络安全解决方案当中，可以提供更为有效的安全性。



Talos 团队介绍

Talos 著名的安全专家团队，由原 Sourcefire 公司的漏洞研究团队，思科威胁智能研究和通讯小组和思科安全应用程序开发小组组成。该团队的专长涵盖软件开发，逆向工程，漏洞分析，恶意软件的调查和情报收集等。Talos 团队同时也负责维护 Snort.org, ClamAV 的, SenderBase.org 和 SpamCop 中的官方规则集和社区。



Talos 的研究成果，将会通过动态的更新，应用于众多的思科安全产品和服务当中，包括业界领先的 ASA+Firepower 下一代防火墙技术，恶意邮件和恶意代码防护技术，Web 安全技术，下一代入侵防御技术以及思科提供的云安全服务技术等，这些技术，可以在多个层面保护思科的用户，在最早的时间，阻挡最新的威胁。前段时间，Talos 团队通过研究分析，发现迄今为止最为复杂的 PoS 系统恶意软件 PoSeidon，并且第一时间在思科的安全产品中提供防御，就是很好的一个例子。