“解读威胁情报，洞悉最新攻击方式，提升高级威胁防御技术”在线研讨会-精彩问答

序号	问题	回答
1	主持人和专家能否介绍详细一点的思科防护网络威胁的产品的具体特点和长处？	思科的威胁防御平台,在全面可见性的基础上, 结合了全球最优的Talos威胁情报, 涵盖了终端/网络/云等各个部分,形成了架构式的威胁防御体系,体系中的各个安全产品,彼此信息共享,策略联动,有效提高了防御的有效性.
2	cisco的沙箱防逃逸有什么技术特点？	Cisco的沙箱把静态分析、动态分析和威胁情报相结合，大多数技术提到的沙箱都是动态分析部分，也就是运行虚拟机模拟运行。Cisco的沙箱会在恶意程序进行动态分析之前，会对恶意程序本身进行静态分析，通过抽取特征和样本进行学习，这个阶段可以检测沙箱逃逸的问题。同时动态分析时结合威胁情报，通过800多个IOC进行多维度分析，提高准确性和命中率。
3	情报取得方式是什么？	Cisco的威胁情报有Talos组织统一进行分析和管理，数据来源有Cisco本身技术收集、第三方合作伙伴和情报分析人员所得，交互方式通过产品的购买和订阅来交付。
4	思科有成熟的数据中心安全防护解决方案么	思科有完整成熟的数据中心安全防护方案,可以参加一下6月14号上午的思科技术达人“秀”- “思科数据中心安全解决方案介绍”
5	cisco 的NGFW 和NGIPS 有什么区别么？和传统的FW IPS相比，感觉很模糊	NGIPS可以是NGFW的一个模块, 也可以独立存在, NGIPS 与传统IPS的主要区别在于:全面的终端/应用可见性的情景感知和智能关联, 动态威胁情报的引入
6	如何得到最新的思科安全消息？第一时间获得新类型漏洞、病毒、攻击的报告或通告	可以关注Cisco的Talos Blog、官方微信、官网发布以及合作伙伴的媒体发布的最新的漏洞和情报通告。

7	沙箱防逃逸有什么技术特点？	沙箱逃逸有几种技术，比如延期执行、检测系统是否虚拟机、Word文件中嵌入黑客PDF文件等，躲避沙箱的动态检测
8	請問內含不作動或已被拆解成分段的惡意程式，丟入沙箱還檢測的到嗎？	在Cisco沙箱的静态分析阶段，可以对文件本身进行分析和检测，如果是拆分分段要看具体情况，有可能无法触发检测条件。
9	我们订购了Firepower 4110，开启这个功能还需要license吗？	对于IPS, 恶意软件防护和URL过滤,需要购买相应的license
10	情报来源很多，有自己检测的有购买交换来的，咱们又是怎么整合在一起的？是否有标准的接口或者格式？	Cisco的威胁情报有Talos组织统一进行分析和管理，数据来源有Cisco本身技术收集、第三方合作伙伴和情报分析人员所得，交互方式通过产品的购买和订阅来交付。
11	情报是否会有分类？例如行业按需来使用，例如有制造行业专有的情报？	情报数据巨大，覆盖率不同行业的漏洞、威胁来源，情报最终在产品订阅中交付，可根据行业特点在产品检测策略中进行分类检测。
12	请问思科针对安全方面有相应的认证么？	Cisco安全的CCIE认证, 针对合作伙伴有Firejumper认证

13	什么时候用threat grid? 如何部署？	Cisco的沙箱是用来检测未知威胁的，把未知的威胁通过分析变成已知，可以和NGFW/NGIPS，WSA，ESA，端点结合，对未知恶意文件进行分析和风险评估，部署模式可以采用本地设备或者云端订阅。
14	攻防演练平台怎么登陆	攻防演练平台无法直接登录,需要与思科的服务部门联系购买
15	CISCO在IPS上有什么新的产品	思科的Firepower平台,可以作为思科新一代的入侵防御平台