在思科安全终端中创建高级自定义检测列表

目录

简介

本文档介绍在思科安全终端中创建高级自定义检测(ACD)的步骤。

背景信息

TALOS Intelligence于2020年1月14日发布了一篇博客，以回应Microsoft星期二补丁漏洞披露。

1月15日更新：为AMP添加了ACD签名，该签名可用于通过伪装成Microsoft ECC代码签名证书颁发机构的欺骗证书来检测CVE-2020-0601的[利用。](#)

在TALOS BLOG中找到的要在ACD中使用的文件的签名：

- Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D020130
- https://alln-extcloud-storage.cisco.com/blogs/1/2020/01/CVE-2020-0601.txt

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

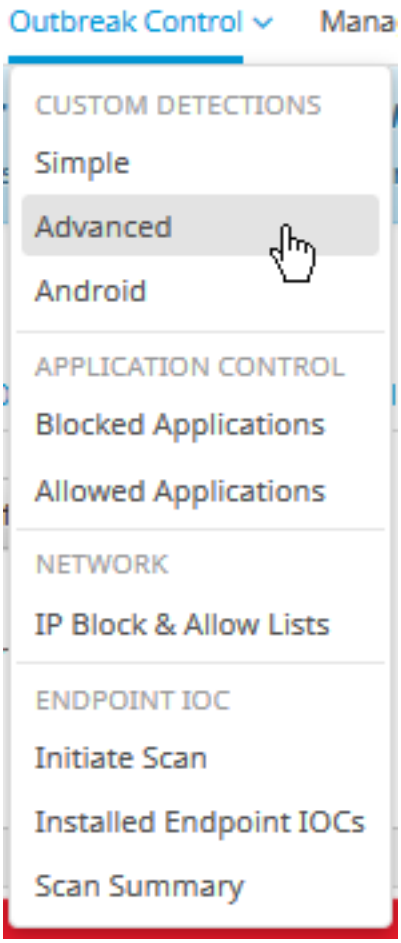
- 思科安全终端云门户
- ACD
- TALOS博客

本文档中的信息在特定实验室环境设备上创建。 所有使用的设备都以已清除（默认）的配置启动。如果您的网络处于活动状态，请确保您了解任何命令的潜在影响。

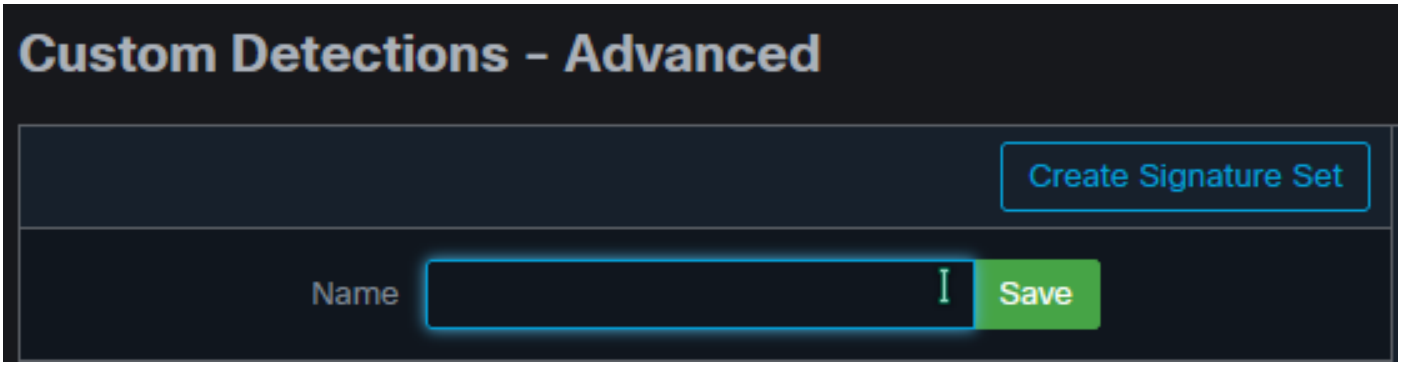
创建高级自定义检测列表

现在，我们创建ACD以进行匹配。

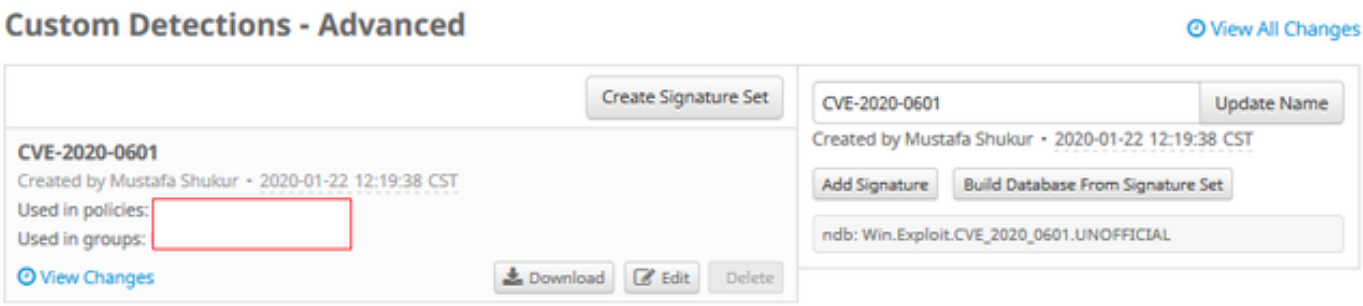
步骤1.导航至**Secure Endpoint Portal > Outbreak Control > Advanced Custom Detection，**如图所示。



步骤2.以签名集CVE-2020-0601的**名称开头，**如图所示。

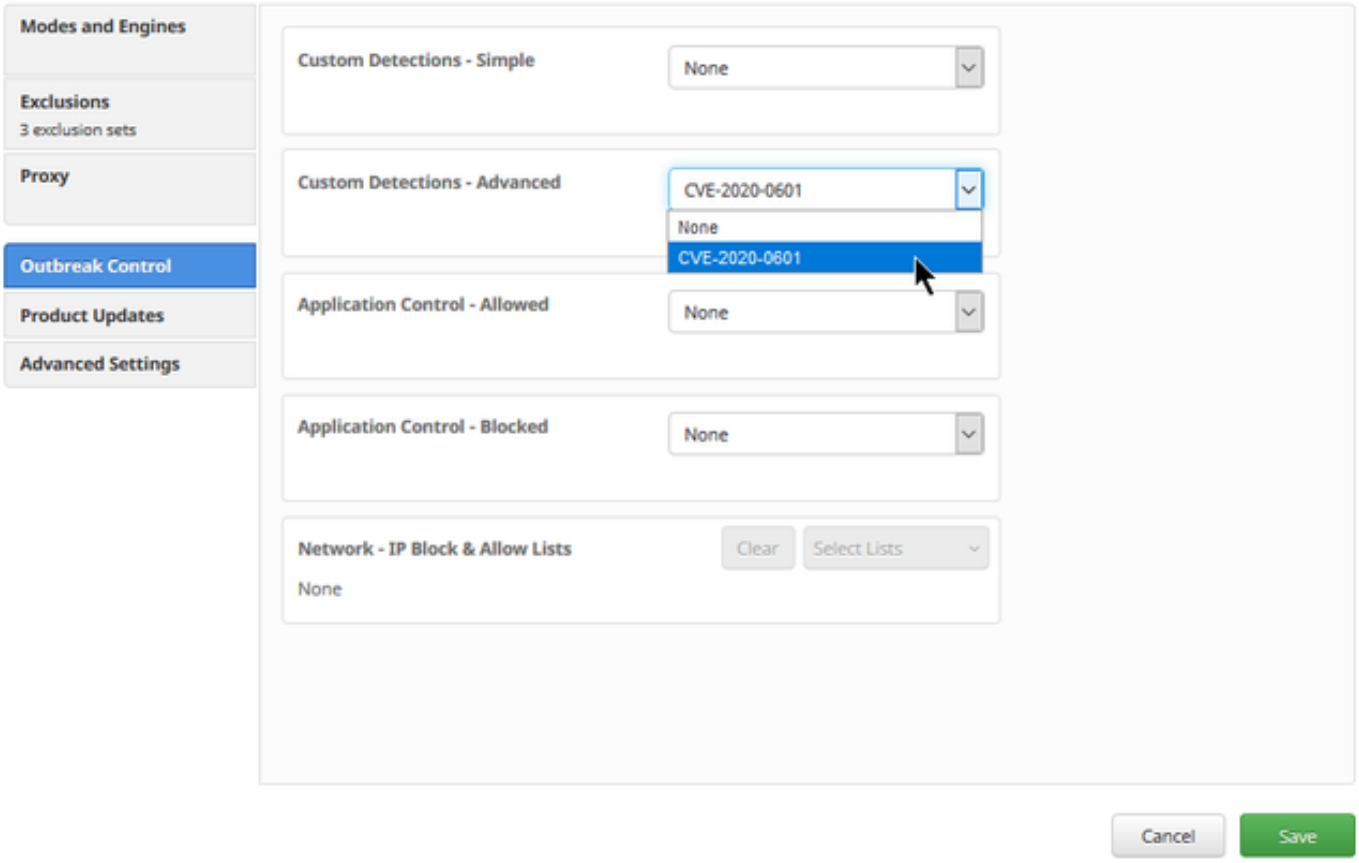


步骤3.接下来，**编辑**该新签名集，然后**添加签名。**
Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D020130。

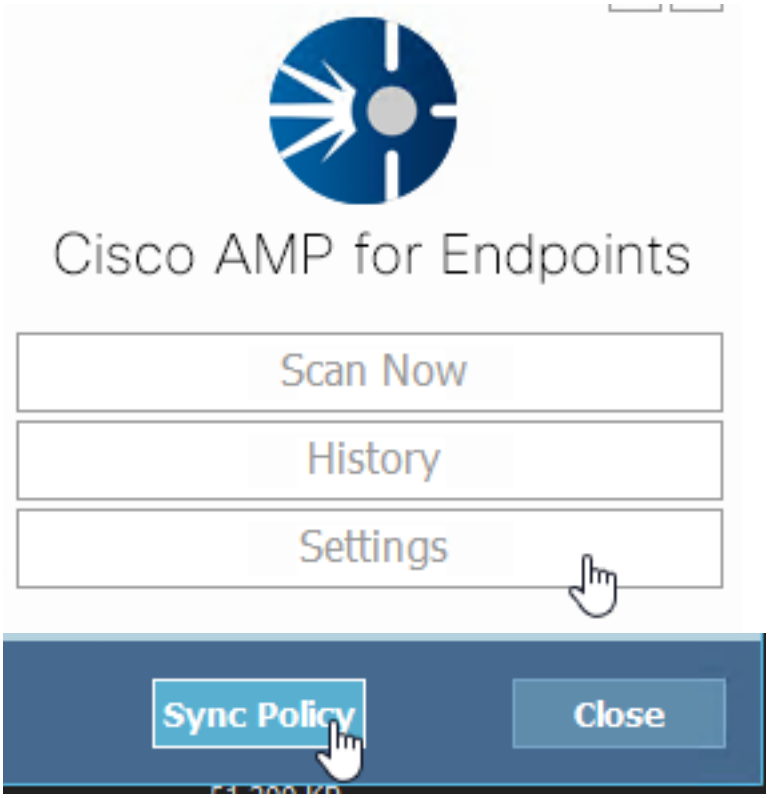


步骤4.选择“**从签名集生成数**据库”，数据库已生成。

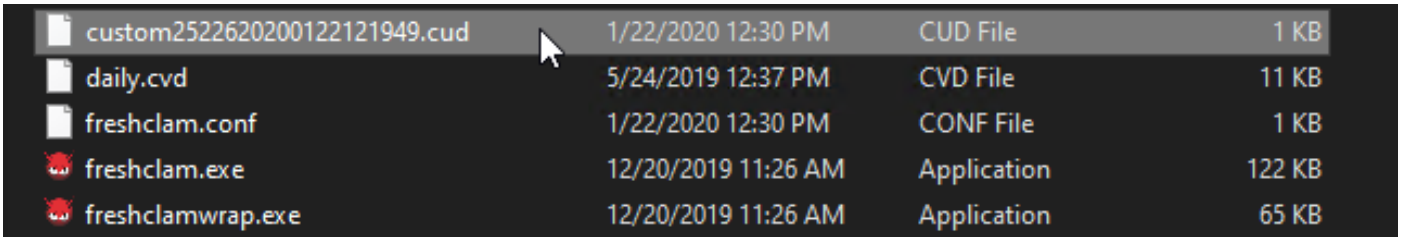
步骤5.将新签名集应用于策略，单击**Edit> Outbreak Control > Custom Detections > Advanced**，如图所示。



步骤6.如图所示，在连接器UI上保存策略和同步。



步骤7.在目录C:\Program Files\Cisco\AMP\ClamAV**中搜**索当天创建的新签名文件夹，如图所示。



相关信息

- 用于测试的生成是Windows 10 1909，不受每个MSKB的漏洞影响；https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601
- https://support.microsoft.com/en-us/help/4534273/windows-10-update-kb4534273
- 适用于：Windows 10、版本1809、Windows Server 1809、Windows Server 2019、所有版本
- **技术支持和文档 - Cisco Systems**