2016 年 12 月 20 日，星期二

IEC 104 协议检测规则

IEC 60870-5-104 协议检测规则

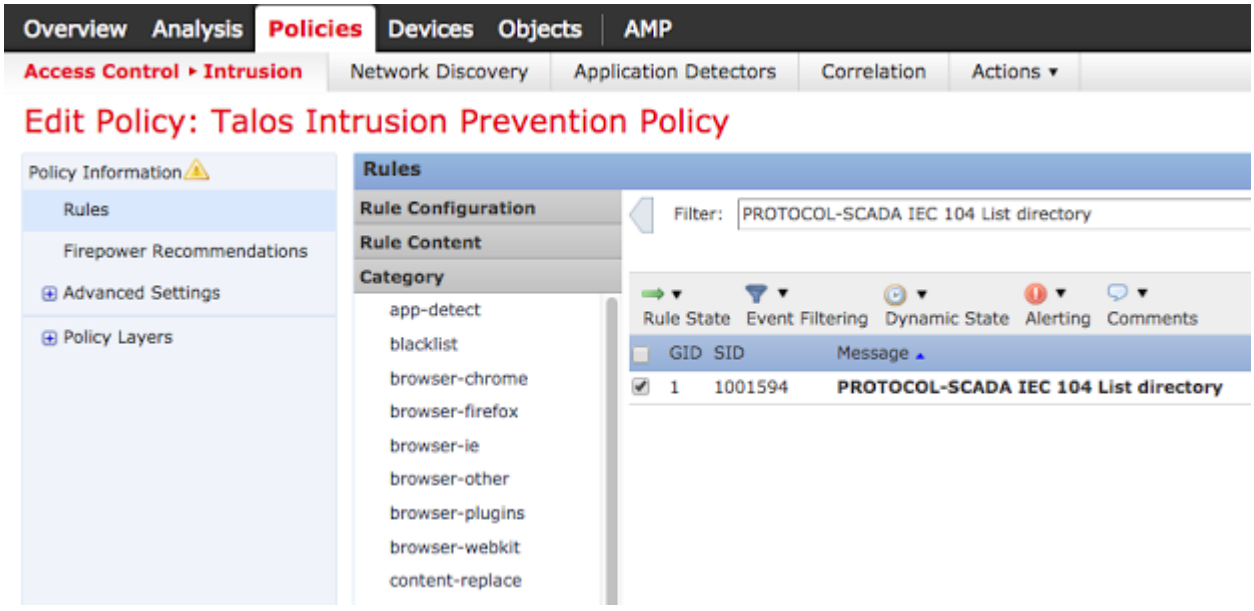
思科 Talos 发布了 33 项用于分析/检查 IEC 60870-5-104 网络流量的 Snort 规则。借助这些规则，工业控制系统/监控和数据采集 (ICS/SCADA) 资产所有者将能够允许对其环境中的正常和异常流量进行识别。

为使这些规则发挥效用，应选择性地打开/启用这些规则。SID 41053 至 41077 用于检测各种 TypeID，如果未使用特定 TypeID，则应启用这些规则。SID 41078-41079 用于检测出入 ICS 网络的 IEC 104 流量。如果 104 流量不应出入 ICS 网络，则应启用这些 SID。

这些规则要求正确配置 Snort $EXTERNAL_NET 和 $HOME_NET 变量，以使某些规则生效。如果网络没有 IEC 104 流量，则不应启用这些规则，因为它们仅用于检测 IEC 104 流量，并可能导致非 IEC 104 流量的误报 (FP)。

什么是 IEC 104？

IEC 104 是 ICS/SCADA 环境中常用的网络协议。各种 ICS/SCADA 设备使用 IEC 104 与其他 ICS 设备通信，包括（但不限于）可编程逻辑控制器、远程终端单元等。



在 FirePower 6.1 中启用 SID

如要阅读有关 snort 博文的更多内容，请点击此处

发布者：WILLIAM LARGENT；发布时间：14:35
标签：ICS、IEC 104、SCADA、SNORT、SNORT 规则、TALOS