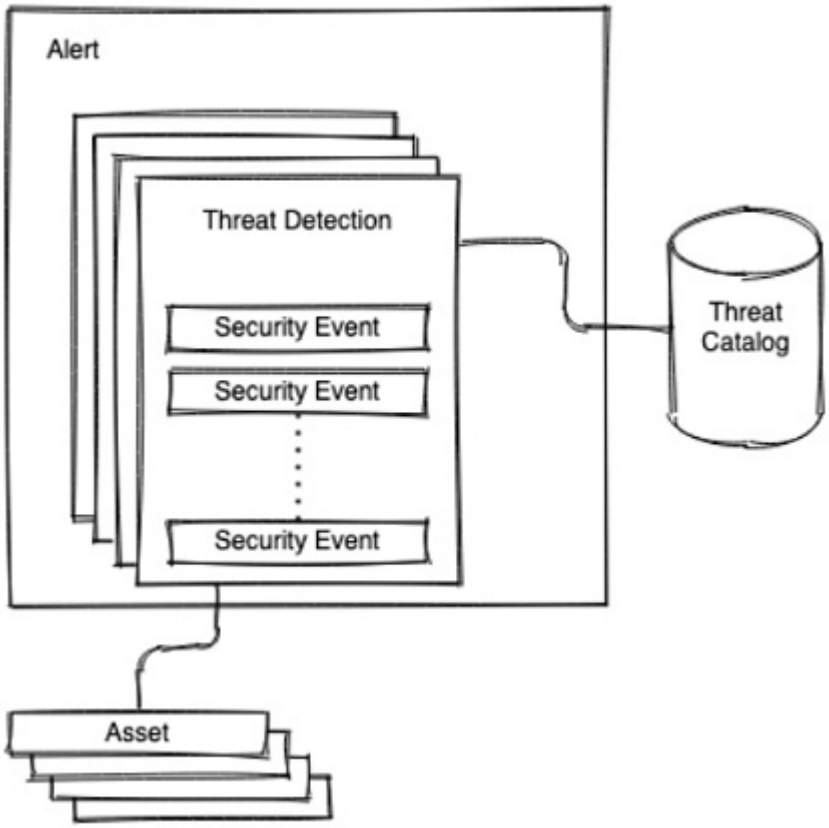
术语表

警报

警报是提示您调查威胁检测的通知。

在全局威胁警报中，警报侧重于一个或多个威胁检测。这些威胁检测发生在一个或多个资产上。我们的融合算法使用这些检测来识别具有相似威胁及其预测的集群，以计算风险级别。然后，我们的 Web 门户会将它们作为安全警报显示在按风险级别划分的优先级列表中。每个警报都指向您的网络上受到的威胁，代表调查和后续补救的自然工作单元。

图 *1:*



安全事件

安全事件是可能表示恶意或可疑行为的重要安全事件。威胁检测引擎用于处理安全事件。对检测可疑或恶意行为至关重要的安全事件称为判定。在威胁检测时为受影响资产观察到的安全事件称为情景。每个安全事件都包含其重要性的说明。此说明称为安全注释。

威胁目录

威胁目录组织了可能的威胁检测，并按三个基本类别进行排序：恶意软件、工具和攻击模式。它还包括到 MITRE 的映射（如果存在）。

威胁检测

威胁检测是指检测影响资产的可疑或恶意行为。在全局威胁警报威胁目录中，它可识别多种类型的威胁检测。

威胁检测引擎可处理各种来源，例如安全事件。它会将它们关联起来，以揭示异常模式和趋势，其可能以一定的置信水平揭示或分析性地证实存在威胁。