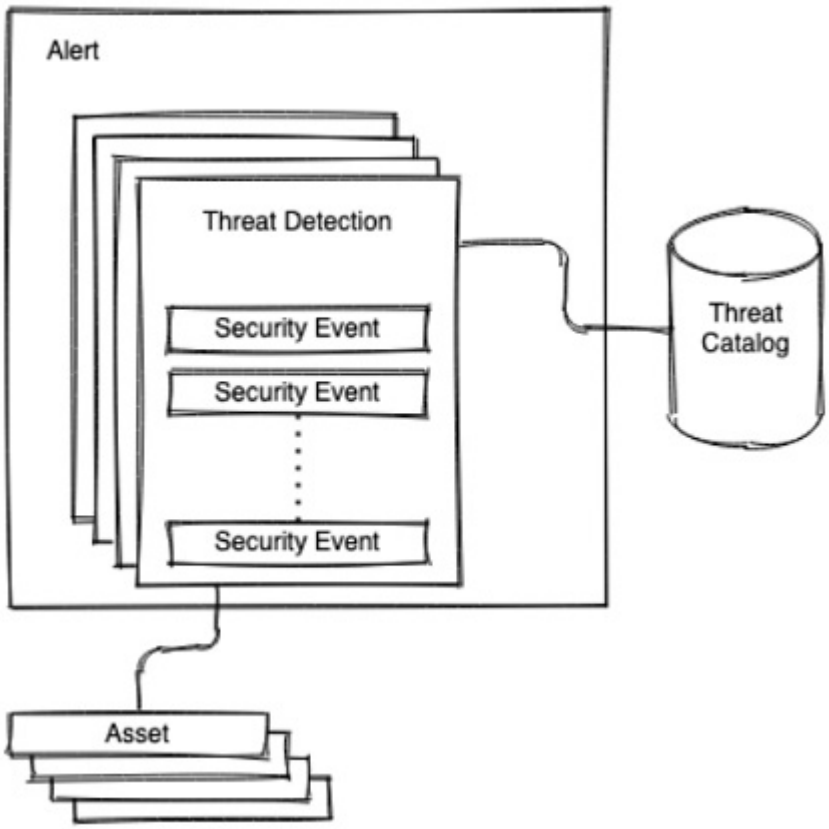
Glossary

alert

An alert is a notification that prompts you to investigate a threat detection.

In global threat alerts, an alert focuses on one or more threat detections. Those threat detections occur on one or more assets. Our fusion algorithm uses these detections to identify clusters of similar threats and their projections to calculate risk levels. Our web portal then presents them as security alerts in a list prioritized by their risk levels. Each alert points to threats on your network and represents a natural unit-of-work for investigation and subsequent remediation.

Figure 1:



security event

A security event is a significant security event that might indicate malicious or suspicious behavior. The threat detection engine processes the security events. Security events that are significant for the detection of suspicious or malicious behavior are called convicting. The security events which are observed for an affected asset in time of threat detection are called contextual. Each security event contains a description of why it is significant. This description is called the security annotation.

threat catalog

The threat catalog organizes possible threat detections and provides their ordering into three basic categories: Malware, Tool, and Attack Pattern. It also includes mapping to MITRE, if it is present.

threat detection

A threat detection is the detection of suspicious or malicious behavior affecting an asset. In the global threat alerts threat catalog, it recognizes multiple types of threat detections.

The threat detection engine works with a wide range of sources such as security events. It correlates them to reveal unusual patterns and trends that potentially reveal or analytically confirm the presence of a threat with a certain confidence level.

threat detection