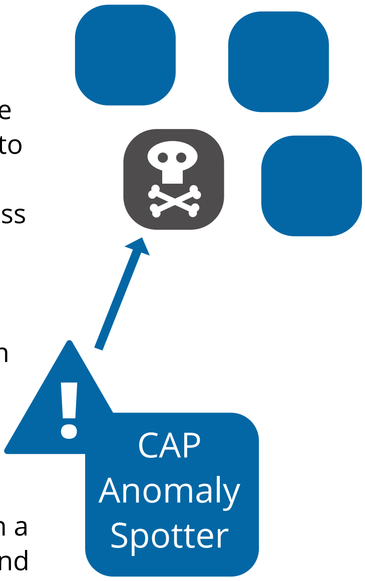
CAP ANOMALY SPOTTER

Anomaly Detection for incident response in IT security

Incident response addresses the aftermath of a security breach or an attack. It is an organized approach that manages these so-called incidents. The primary goal is to limit damage and reduce recovery time and costs after the situation. An incident response plan is a policy that helps to address an incident. Such a plan usually defines what constitutes an incident and, in addition, describes a process that should be followed when an incident occurs.

Incident response is one of the key service offerings of IT security service providers, often an operational element in a Security Operation Center (SOC). Incident response is conducted by highly professional IT security experts equipped with a wide selection of tools. These data collection and monitoring tools record various endpoint and network events in detail, and store this information in a database for detection, analysis, investigation reporting and alerting.



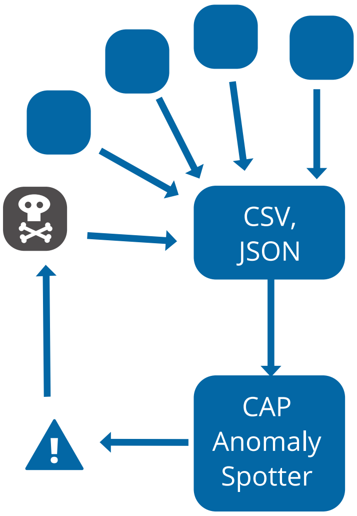
Opportunity for advanced machine learning analytics in incident response

The critical part of the incident response operation is the so-called triage phase. During the triage stage the goal is to determine as quickly as possible the compromised computer(s) based on post-collection analysis of the data gathered from the devices over a long time period.

Case: CAP Anomaly Spotter for incident response

Company: A global IT security service company

The challenge: Our customer wants to improve the response time in the triage stage with a tool that detects computers that seem to be behaving in a suspicious manner and thus, are potential cause for the security incident. Anomaly detection techniques using advanced machine learning intelligence is a natural choice in such applications.



Our solution: We adopted CAP Anomaly Spotter engine to the specific use cases and the specific data format used by our customer. Our customer applies its proprietary method in collecting, storing and consolidation of the data and provides the data to CAP Anomaly Spotter in CSV, JSON or in a similar format. CAP engine processes the data and, in particular, detects anomalies that are known to indicate a possible cause for a security incident, such as computers communicating to unusual destinations or processes running in computers that deviate from normal operations. The objective of the analysis is to narrow the number of computers to a manageable level for further detailed investigation, and in this manner, speeds up the critical phase of the incident response process.

Benefits of CAP Anomaly Spotter

- Cuts the time of the triage phase in IT incident response operations.
- Makes possible quicker sanitation operations and thus limits the damage caused by the incident.
- Works seamlessly with other tools and processes used in incident response operations.
- Improves efficiency and decreases the cost of incident operations

About CAP Data Technologies

CAP Data Technologies is a Finnish technology startup providing data analytics solutions utilizing our advanced anomaly detection technology. CAP Anomaly Spotter has the ability to detect previously unknown behavior in the system without relying on pre-set rules or fingerprints.

Contact CAP Data Technologies

tuomo.sipola@capdatatechnologies.com	tel: +358 40 753 2169
markku.ranta@capdatatechnologies.com	tel: +358 50 324 6233

Try out the free trial version on our web site
www.capdatatechnologies.com