CYBRAICS

Persistent Behavior Tracing (PBT)

The Challenge

Cyber threats increasingly exploit gaps in an organization's security posture created by siloed data pools of security products and the challenges associated with query-based analysis. Query-based analysis requires large amounts of data to be online or restored from backups to search.

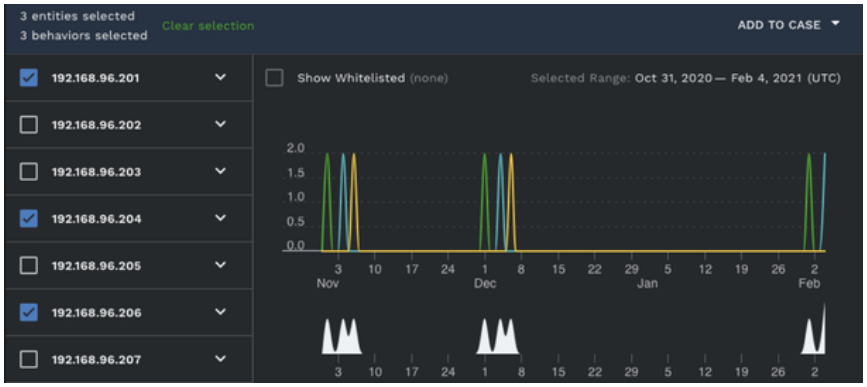
The Solution

Cybraics has a unique method of storing deduplicated behavior attributes associated with each event on a per entity basis. This allows for a historical contextual view over an unlimited timeframe without massive storage requirements.
We call it Persistent Behavior Tracing (PBT).

Find Threats Others Miss, Fill Gaps In Your Security Posture

PBT utilizes a unique hash sum, calculated at processing time, from fields describing each behavior. PBT identifies behaviors via a variety of detection methods determined by the analytics that generate that behavior and each occurrence of a behavior is then tracked using a set of fields specific to that behavior. The result is a system that tracks attack vectors in real-time, saves relations indefinitely, and identifies associations based on the threat behavior.

Persistent Behavior Tracing (PBT) Example
Web Server Attack, Multiple Source IPs



197 Days
average time to detect a breach [1]

Identify correlations between threat signals over all time

Eliminate extensive and expensive log management hot storage requirements

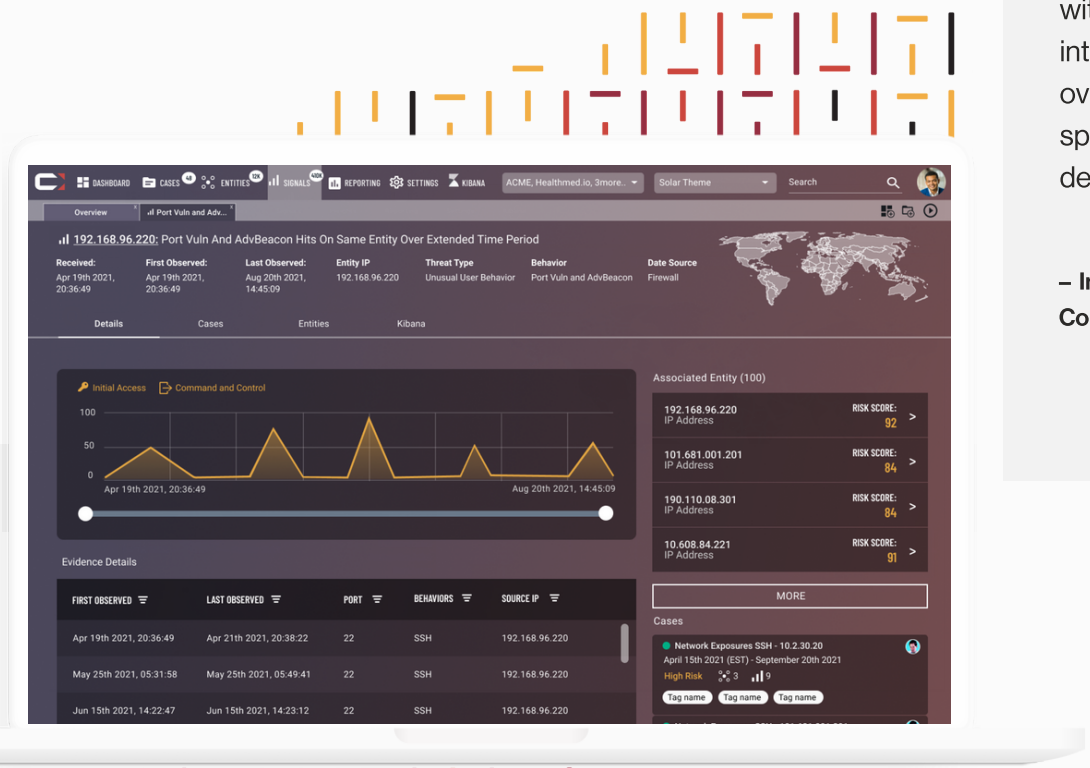
Streaming analytics identify threats in real-time vs. batch processing

Dramatically increase security analyst accuracy and efficiency

Increase Analyst Efficiency and Reduce Storage Costs

Analysts spend an extraordinary amount of time investigating suspicious activity. Traditional SIEM and even SOAR products treat alerts and events in isolation and utilize batch processing. PBT eliminates the need for manual queries and accelerates resolution with historical contextual views with all the relevant attributes in a single dashboard.

Organizations often have to weigh the benefit of maintaining vast amounts of log data in hot storage versus the incurred cost of that storage. PBT's unique hash sum deduplication eliminates the need for massive volumes of expensive hot storage. PBT also eliminates the need for backup-restores and the delays and complexity associated with them. This opens up the window for investigation and research since there are no disruptive, complex and time-prohibitive delays that prevent analysts from fully researching potential threats.



> Leveraging Artificial Intelligence and Machine Learning is the only way to have a shot at analyzing the mountains of data coming from so many different systems.
>
> Analyzing and correlating event logs with the necessary intelligence is long overdue in the security space and Cybraics delivers."
>
> **– International Media Company**

(1) 2021 IBM/Ponemon Institute Cost of a Data Breach Report

Cybraics.com

2400 East Commercial Blvd.
Suite 215, Ft Lauderdale, FL
33308

Cybraics was developed out of a long-term, award-winning machine learning and AI research program designed to support the U.S. Department of Defense. With the rigorous demands of national defense as our foundation, we've continued to improve and evolve our nLighten™ platform to be the world's leading autonomous SIEM and MDR solution, with proven success across industries like energy and entertainment, finance to healthcare, government to education and more.

See Cybraics nLighten in action with a personalized demo or give us a call at (844) 283-0458.