SOLUTION BRIEF

Persistent Behavior Tracing (PBT)

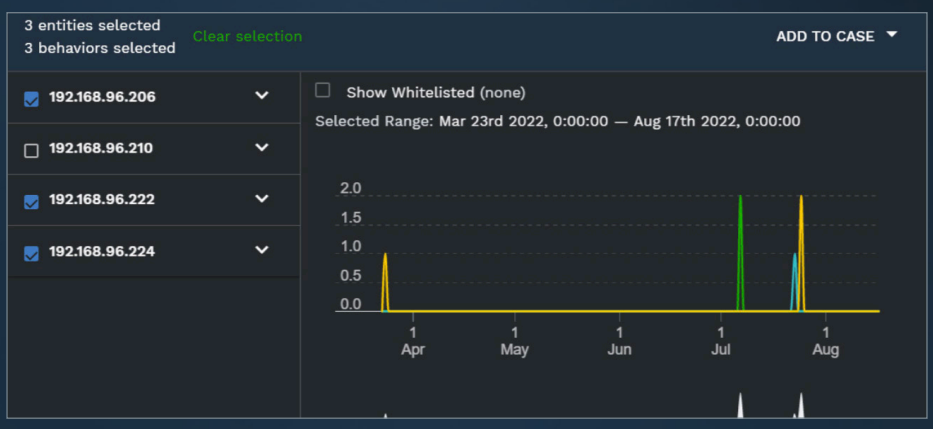
Cyber threats increasingly exploit gaps in a healthcare organization's security posture created by isolated data pools of security products and the challenges associated with query-based analysis. Query-based analysis requires large amounts of data to be online or restored from backups to search.

PatientLock has a unique method of storing reduplicated behavior attributes associated with each event on a per entity basis. This allows for a historical contextual view over an unlimited time 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

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

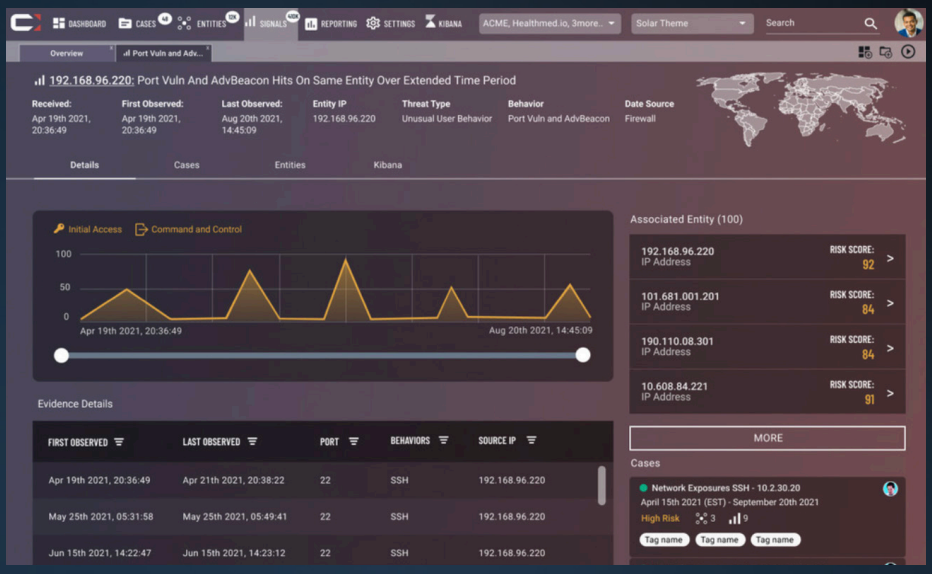
Dramatically increase security analyst accuracy and efficiency

SOLUTION BRIEF

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.

Healthcare organizations are often forced 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 reduplication 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 the window for investigation and research since there delays preventing analysts from researching potential threats.



> Leveraging Artificial Intelligence and Machine Learning is the only way to even have a shot at analyzing the mountains of data coming from so so many different systems.
>
> Analyzing and correlating event logs with the necessary intelligence is long overdue in the security space, and this delivers.
>
> - Gus Savloff
> EyeMD EMR

Call PatientLock 866-938-4250

linkedin.com/company/patientlock

twitter.com/patientlock

www.patientlock.net

866-938-4250
info@patientlock.net

Corporate Woods - Building 51
9393 W. 110th Street, Ste. 500
Overland Park, KS 66210