SOLUTION BRIEF

DC Consulting

Managed Security Services powered by SILVERSKY

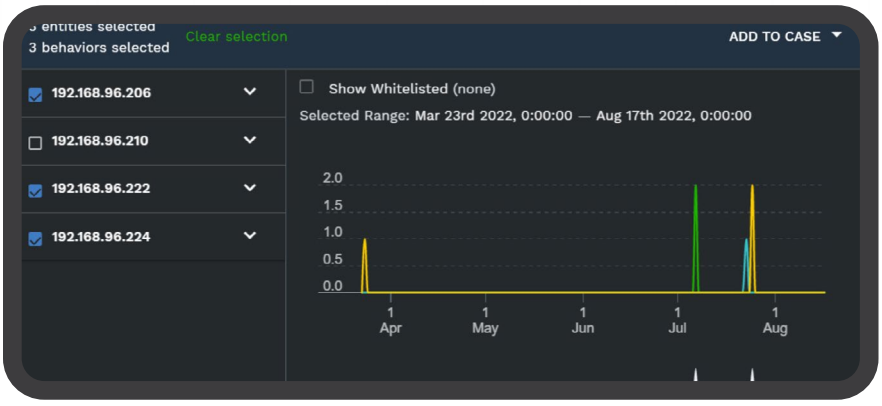
PERSISTENT BEHAVIOR TRACING (PBT)

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.

DC Consulting Managed Security Services, powered SilverSky, has a unique method of storing de-duplicated behavior attributes associated with each event on a per entity basis. This allows for a historical contextual view over an unlimited time frame 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

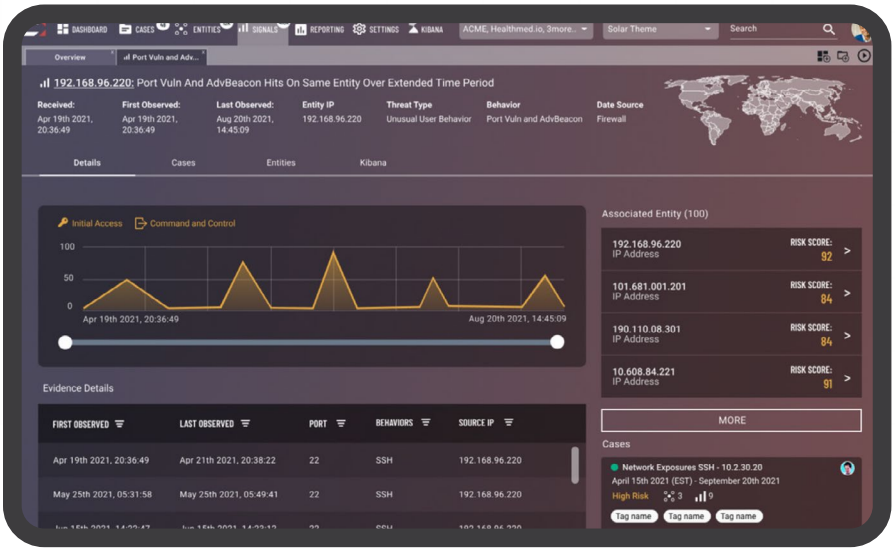
Dramatically increase security analyst accuracy and efficiency

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.

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 de-duplication 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.



About DC Consulting

DC Consulting is a leading provider of cybersecurity and digital infrastructure solutions. Through security analytics, AI, and detection solutions, we help you know and sense your enemy before they strike. Through assessments aligned with industry standard security controls and frameworks, we ensure you have visibility into your organization's overall risk exposure. We ensure our clients stay on the bleeding edge of innovation by embracing proven, disruptive technologies that counter both known and unknown threat vectors.

866.372.0213 | sales@dcconsulting.com | www.dcconsulting.com

DC Consulting
Managed Security Services powered by
SILVERSKY