SOLUTION BRIEF

Persistent Behavior Tracing (PBT)

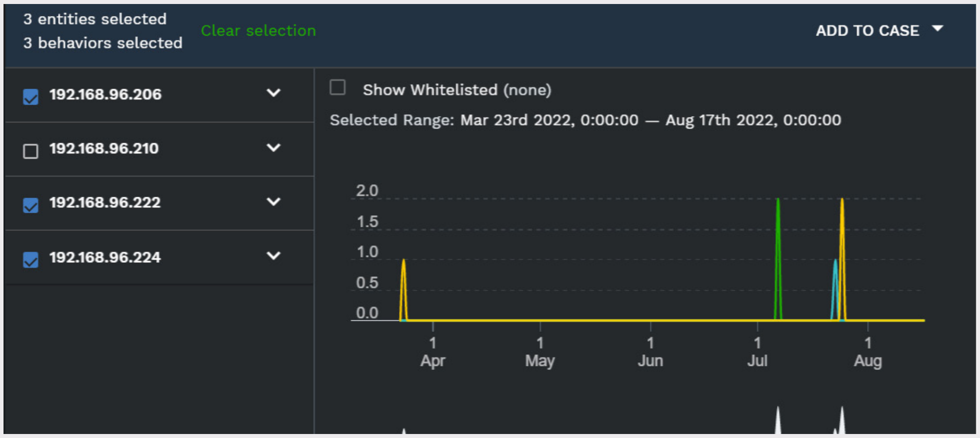
Cyber threats increasingly exploit gaps in an organization's security posture created by siloed data pools of security products and the challenges associated with query-based analysis. Query-based analysis requires large amounts of data to be online or restored from backups to search.

SilverSky 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



3 entities selected
3 behaviors selected

☑ 192.168.96.206
□ 192.168.96.210
☑ 192.168.96.222
☑ 192.168.96.224

□ Show Whitelisted (none)

Selected Range: Mar 23rd 2022, 0:00:00 — Aug 17th 2022, 0:00:00

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

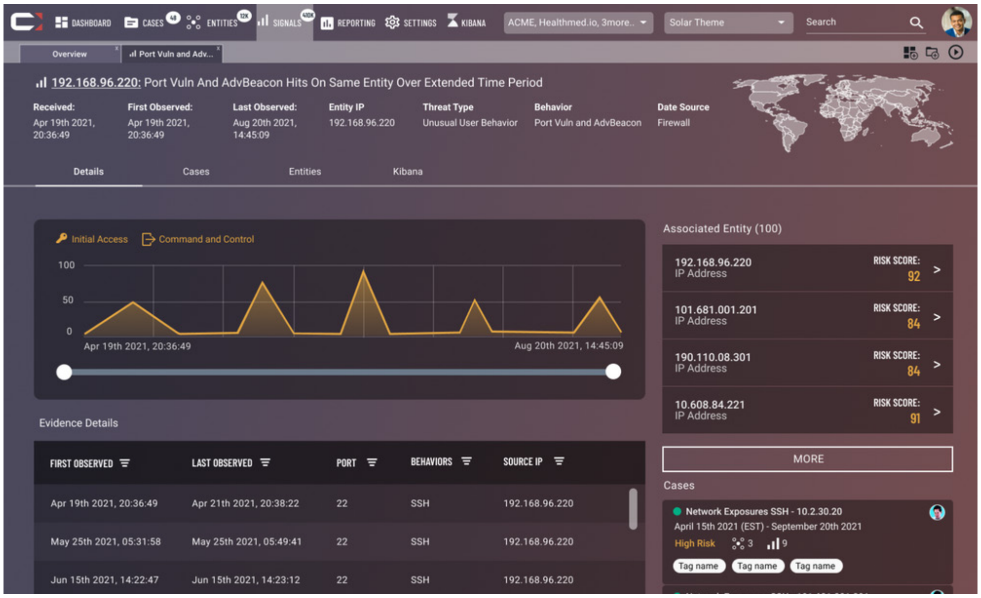
Streaming analytics identify threats in real-time vs. batch processing

Dramatically increase security analyst accuracy and efficiency

Increase Analyst Efficiency and Reduce Storage Costs

Analysts spend an extraordinary amount of time investigating suspiciousactivity. Traditional SIEM and even SOAR products treat alerts and events inisolation 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.



192.168.96.220: Port Vuln And AdvBeacon Hits On Same Entity Over Extended Time Period

Received:	First Observed:	Last Observed:	Entity IP	Threat Type	Behavior	Date Source
Apr 19th 2021, 20:36:49	Apr 19th 2021, 20:36:49	Aug 20th 2021, 14:45:09	192.168.96.220	Unusual User Behavior	Port Vuln and AdvBeacon	Firewall

Evidence Details

FIRST OBSERVED	LAST OBSERVED	PORT	BEHAVIORS	SOURCE IP
Apr 19th 2021, 20:36:49	Apr 21th 2021, 20:38:22	22	SSH	192.168.96.220
May 25th 2021, 05:31:58	May 25th 2021, 05:49:41	22	SSH	192.168.96.220
Jun 15th 2021, 14:22:47	Jun 15th 2021, 14:23:12	22	SSH	192.168.96.220

Associated Entity (100)

192.168.96.220 IP Address	RISK SCORE: 92
101.681.001.201 IP Address	RISK SCORE: 84
190.110.08.301 IP Address	RISK SCORE: 84
10.608.84.221 IP Address	RISK SCORE: 91

Cases

Network Exposures SSH - 10.2.30.20
April 15th 2021 (EST) - September 20th 2021

> "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 SilverSky delivers.
>
> **– International Media Company**"

Call SilverSky
1-800-234-2175

SilverSky

1-800-234-2175
learn@silversky.com

3015 Carrington Mill Boulevard
Suite 400
Morrisville, NC 27560

linkedin.com/company/silversky
twitter.com/SilverSky
www.silversky.com