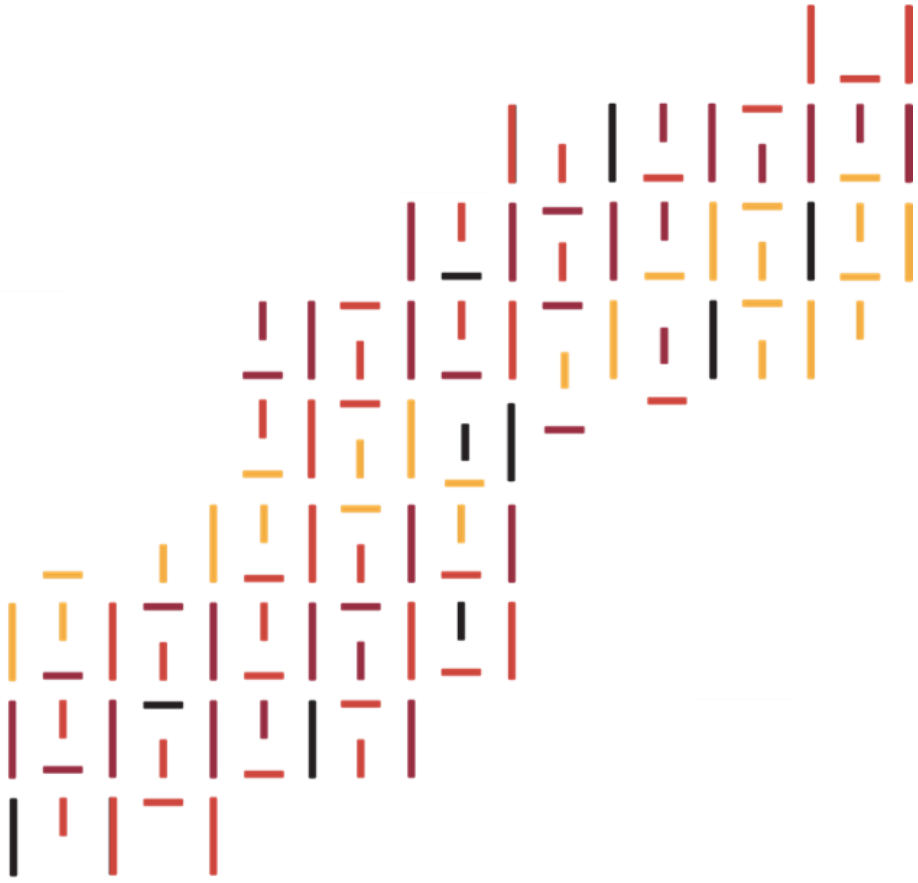
CYBRAICS



nLighten™

Cybraics Persistent Behavior Tracing

CYBRAICS

TABLE OF CONTENTS

OVERVIEW

Cybraics has a unique method of storing unique traced behaviors in a relational database. This method solves one of Cyber Security's biggest problems: gain historical context of behaviors over unlimited timeframe, show linkages between similar entities while not losing relevant context which would require analysts to go back to querying raw logs.

Similar products (e.g. Splunk, QRadar, Vectra Ops, ArcSight, Exabeam, etc.) in the SIEM or log management market are leveraging the traditional query-based approach to retrieving data. They all require that large amounts of data remain online and queryable, often requiring backup restoration to view data that has been archived to reduce storage costs. This is a time-consuming process and thus often skipped by security analysts due to time constraints during investigations.

Hashing of fields is sometimes used during case investigations but has never used to define all behaviors in the system.

PERSISTENT BEHAVIOR TRACING DEFINITION

Cybraics has developed a new feature called "Persistent Behavior Tracing" that can intelligently track behaviors found in logs over unlimited timeframe and across multiple entities (entities are objects you can attribute behaviors on e.g. IP address, Username or Host name). This unique capability allows nLighten to store each behavior only once, aggregate a count for number of occurrences, allowing for historical contextual view, and extracting relevant attributes required for the analyst to make sense of the event. This feature saves the security analyst significant time in identifying unusual events and provides instant correlation between multiple entities.

Cybraics' Persistent Behavior Tracing method is fundamentally different from storing individual behaviors using traditional log management databases. A behavior trace is a unique hash sum, calculated at processing time, from fields describing each behavior. Our method does not use conventional fingerprinting, in which log lines are flagged based on simple pattern matching. Instead, behaviors are identified via a variety of methods which are determined by the analytics generating the behavior, and each occurrence of a behavior is tracked using a set of fields specific to the behavior. This historical view of the behavior is available for analysts even after the original logs have been archived.

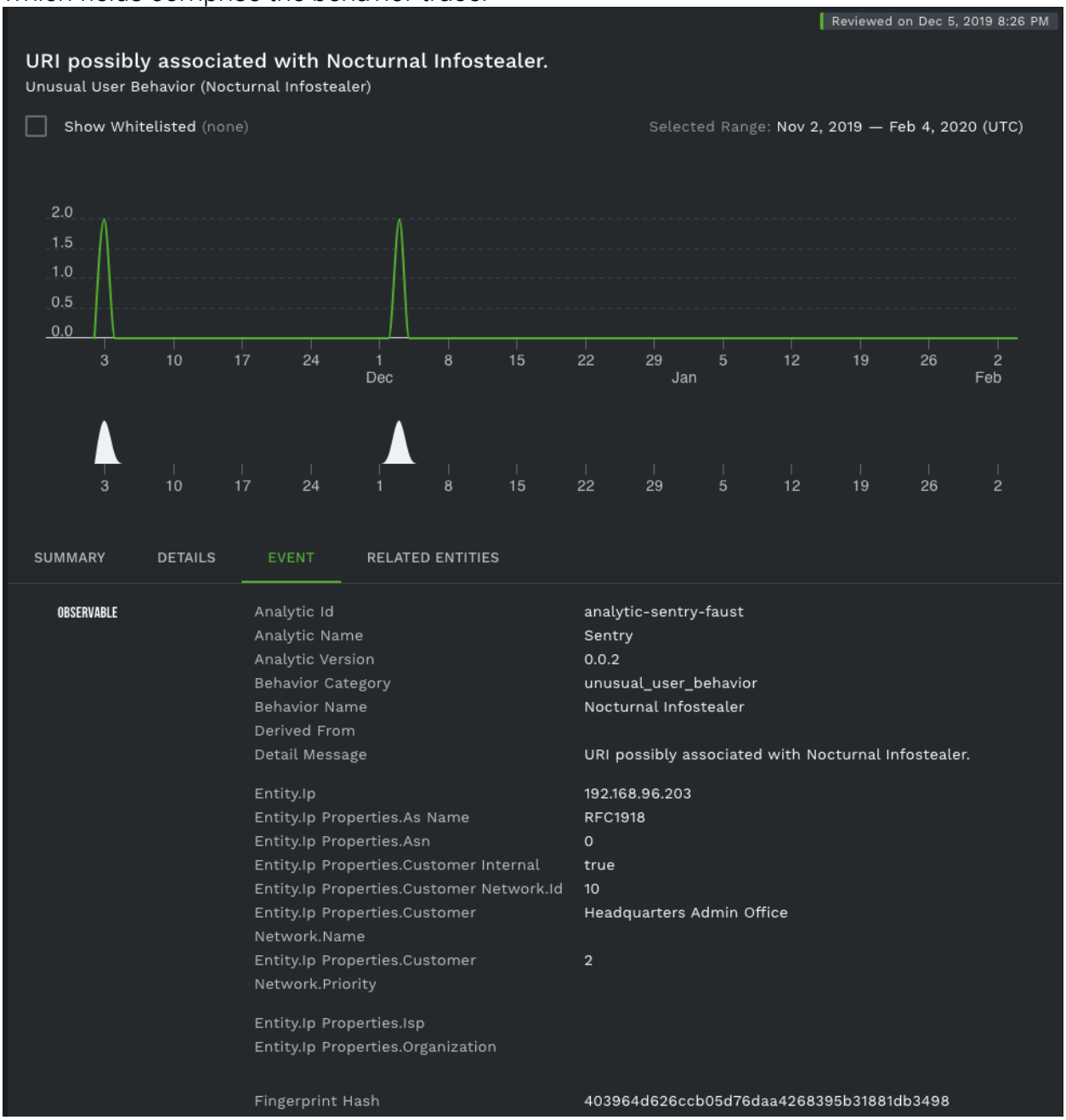
A key differentiator to our method of fingerprinting is that we store de-duplicated behavior attributes to each event on a per entity basis. This is very useful when looking at specific attack vectors such as not only tracing a Web server attack but also showing first and last seen of each file being attacked.

Example:

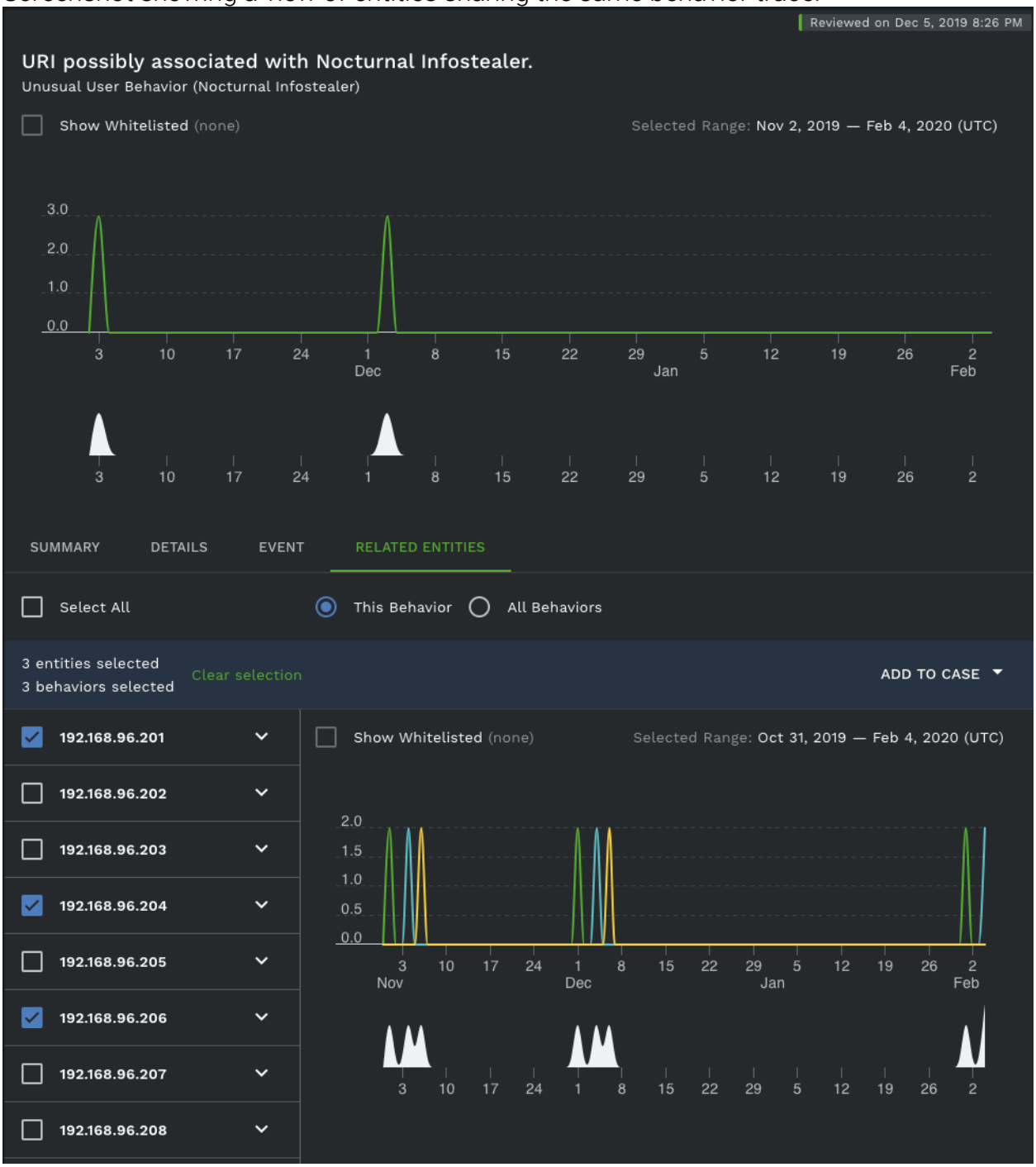
Web server attacks happen frequently. An advanced attacker typically switches source IP addresses to trick conventional tools and analyses. In our method of Persistent Behavior Tracing, we can save the attack vector fields, and also show which pages were attacked. This means that the security analyst does not have to query logs to gain insight on the

attack vector. The analyst can retrieve a list of all entities performing similar attacks, regardless of the easily changed source IP address.

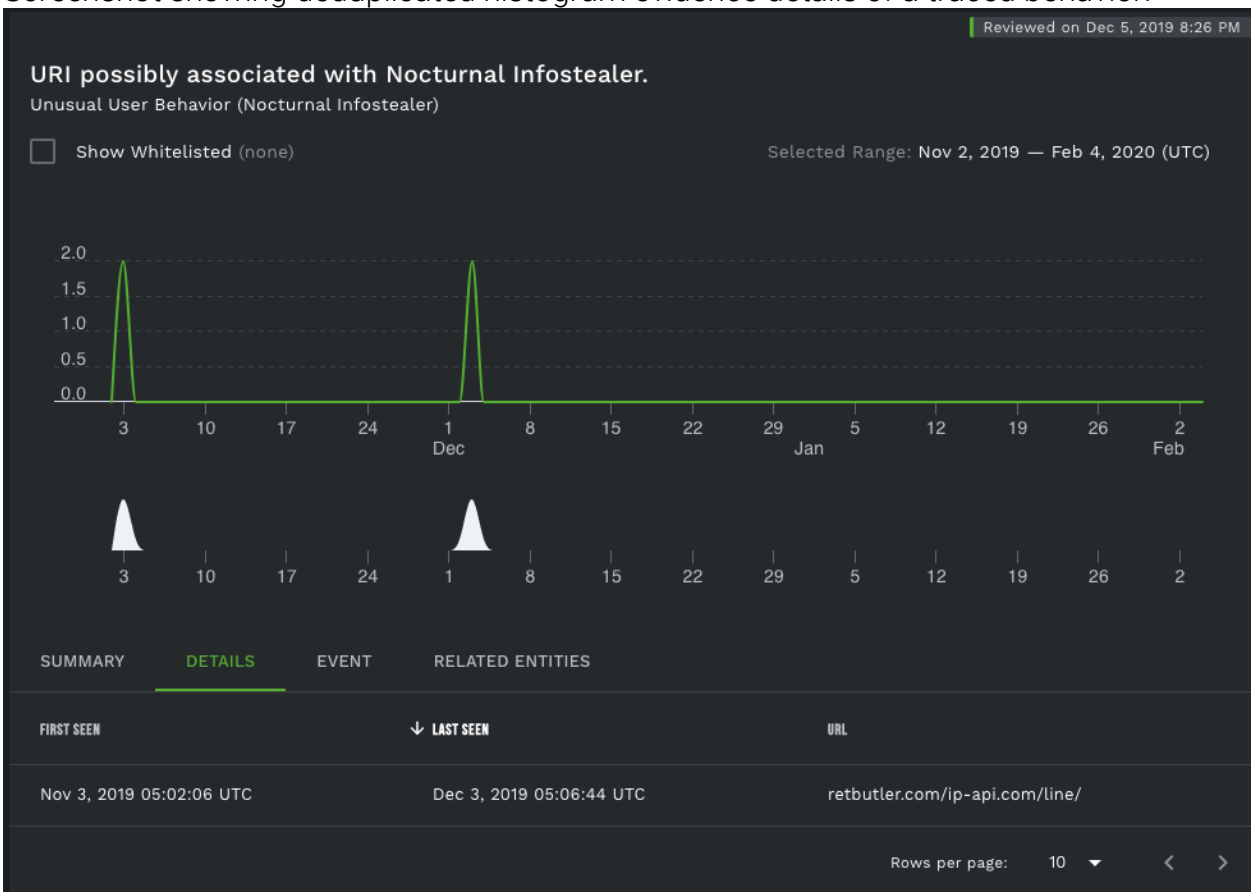
This screenshot shows a behavior history in a graphical timeline, as well as a detailing of which fields comprise the behavior trace.



Screenshot showing a view of entities sharing the same behavior trace.



Screenshot showing deduplicated histogram evidence details of a traced behavior.



Note: same URL was first detected on Nov 3 and most recently on December 3.

KEY BENEFITS

Cybraics' method for Persistent Behavior Tracing provides several benefits, listed below.

Increased security analyst efficiency (timesaving and increased efficiency)

Security analysts spend a lot of time investigating suspicious activity. In traditional SIEM tools they often will need to re-do these investigations as they have no historical view of the data. Performing long-term searches are often not done or only done during critical investigations as they can take a long time to complete, sometimes requiring restoration of backed up logs and often require several complex queries to complete. These advanced queries are difficult to compose, and most analysts do not have experience or training or time to fully research suspected suspicious activities.

Persistent Behavior Tracing solves this issue because all the information the analyst would need is readily available: historical context, significant evidence details and relationship with other entities.

Reduced storage cost

Storage is the largest cost when implementing traditional SIEM or Log Management solutions. Companies often need to weigh the benefit of maintaining vast amounts of logs

online vs. the incurred cost. Companies are forced to store logs by certain compliance frameworks and certain companies minimize the logging by systems to reduce those costs. These issues contribute to higher risks of a security event, and the difficulty in determining the initial issue and finding all of related evidence that led to a breach, as well as the extent of the breach.

Persistent Behavior Tracing reduces the requirement to have a large timeframe of logs online. Through the use of evidence details, context is available that would otherwise require the logs to be online during investigations. This substantially reduces the storage cost and the retrieval efforts and enables companies to have instant visibility into anomalous attacker behaviors.

PERSISTENT BEHAVIOR TRACING IS NON-OBVIOUS

Cyber Security has been dominated by the requirement to store vast amounts of logs online, required for conventional platforms to have available for manual searches for attacker behaviors. Companies like Exabeam now require the customer to take over all the storage cost while they charge a flat fee for their platform, others like Splunk have complex calculators to determine costs for “hot” (fast storage), “warm” (slower, cheaper hard drives) and “cold” (offline, backed up) storage. This is because they have not figured out how to store unique behaviors without losing the context that our Persistent Behavior Tracing advancement allows for in the evidence details fields.

There is an opportunity cost associated with traditional platforms in this area. The complex search language queries required to be written and leveraged by experts is not pervasively used and thus puts companies at increased risk. Companies that leverage Persistent Behavior Tracing can now instantly find anomalous behaviors in vast amounts of log data as well as similar behaviors that normally cannot be easily identified. This allows the security analyst to address remediation efforts sooner, and focus on all of the related events, thus significantly reducing risk and saving time and money.