APPLICATION NOTE

THREATQUOTIENT™

# MAXIMIZE SIGNATURE VALUE AS PART OF THREAT OPERATIONS

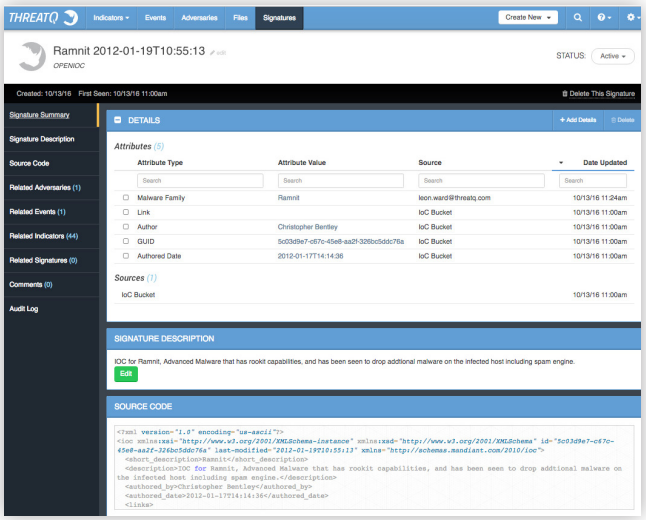
The true value of a signature comes from the context provided along with its detection. How that data is presented is maximized inside ThreatQ™.

This document introduces the importance of signature processing to maximize value in a company's threat operations and management program, and how the ThreatQ™ Threat Intelligence Platform enables that process.

## WHAT'S BEHIND A SIGNATURE?

A good signature contains compound statements for the detection of an object or event, along with supporting information that describes what has been observed when that signature "fires" (creates an event).

In a threat intelligence context, a signature can contain a wealth of data to better understand your attacker, the methods they employ, and the toolset they use. Therefore, it's vital that a threat intelligence platform can fully decode a signature to extract all indicators and the related contextual attributes. Without this context, the indicators are just pieces of data vs. the intelligence needed as part of threat operations.




*A "fully decoded" OpenIOC signature in ThreatQ, along with 44 indicators that were automatically found and extracted.*

### EXTRACT INTELLIGENCE FROM SIGNATURE CONTENT

- Decode signature content automatically
- Extract and link indicators and attributes

### ACCELERATE HUMAN ANALYSIS

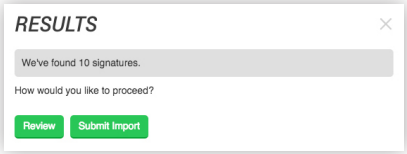
- Display signature attributes that are automatically decoded
- Understand the motivation behind a signature
- Provide syntax highlighting for easy consumption

### PUBLISH AN OPTIMAL SIGNATURE SET

- De-duplicate imported signatures
- Combine signature intelligence across sources and formats
- Build signature sets that are relevant to your adversaries

During the import process, additional context about the signatures can be added, as well as links made to events, adversaries or any other objects found inside ThreatQ.

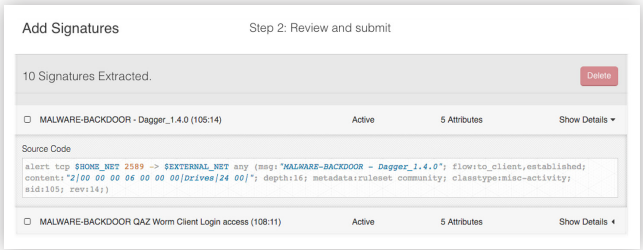
Some signature languages can be complex to read and understand. ThreatQ decodes a signature by presenting the core information about it in an easy-to-consume manner, with attributes, names and descriptions all automatically created from the signature content. This accelerates how quickly you can understand the motivations behind what the signature is looking for and, more importantly, why.




The signature import process is optimized based on the volume and type of signatures being uploaded. If a file contains multiple signatures, each signature is individually extracted, named, decoded and saved as its own record within ThreatQ. This process ensures that signature content can be aggregated and linked just like any other intelligence object.

Storing each signature separately is vital for when the signature content is to be exported for use inside the sensor grid. Without separate storage, it is impossible to export the specific signatures you need or prevent the export of duplicates that will likely result in broken configurations.

ThreatQ provides powerful export functions that can be accessed via the GUI or the RESTful API to use in your detection tools or to share content between different groups. Export capabilities include native signatures from the platform, as well as the ability to automatically convert and export indicators into signature formats.




*Reviewing a Snort "rules" file where each signature has been extracted for storage as its own object.*

## SIGNATURE PROCESSING AT A GLANCE

- Extract signatures from uploaded files and store them as unique objects
- Decode signature content and extract attributes for context
- Detect & extract indicators that may be embedded in the signature
- Link signatures to adversaries, events, campaigns and evidence files, like PCAPs
- Track changes to the signature and its relationships with a full audit log
- Auto-generate signatures from indicators within the system
- Export functions based on attributes associated with them, for example:
  – Export all Snort signatures related to: "adversary name," "Kill Chain phase," "Malware family," etc.
- Full RESTful API Access to signatures
- Enables tighter collaboration between signature and intelligence team

## DON'T BE FOOLED BY OTHER APPROACHES

- Simply storing a text object as a signature loses vital context
- Without breaking apart and parsing signature files during import, it's impossible to treat each signature as its own entity
- De-duplication of and aggregation of signatures is important to ensure quality exports to the sensor grid
- Without automated extraction of indicators from signatures, additional links to adversaries and more context will be lost

## ABOUT THREATQUOTIENT™

ThreatQuotient understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, empowers defenders to ensure the right threat intelligence is utilized within the right tools, at the right time. Leading global companies are using ThreatQ as the cornerstone of their threat intelligence operations and management system, increasing security effectiveness and efficiency.

For additional information, please visit threatq.com.





THREATQUOTIENT™
11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • Sales and General Inquiries: +1 703 574-9885