Next level threat hunting

If only I could hunt across my entire environment...

Challenges facing threat hunters are no joke, and hunt teams face a number of challenges in trying to identify meaningful signals to uncover the unknown, like:

Partial visibility and limited retention
Hunters are unable to get a clear picture to conduct a hunt due to different systems involved and the data or files are no longer available; limited data is available or incomplete.

Manual triaging and correlating threat intel
Significant time and effort is needed to manually correlate the intelligence received and extrapolate into meaningful signals.

Limited queries and access is restricted
Hunters can't run queries in the way needed across their organization. Instead, they have to run queries on multiple systems and then try to piece them together after the fact.

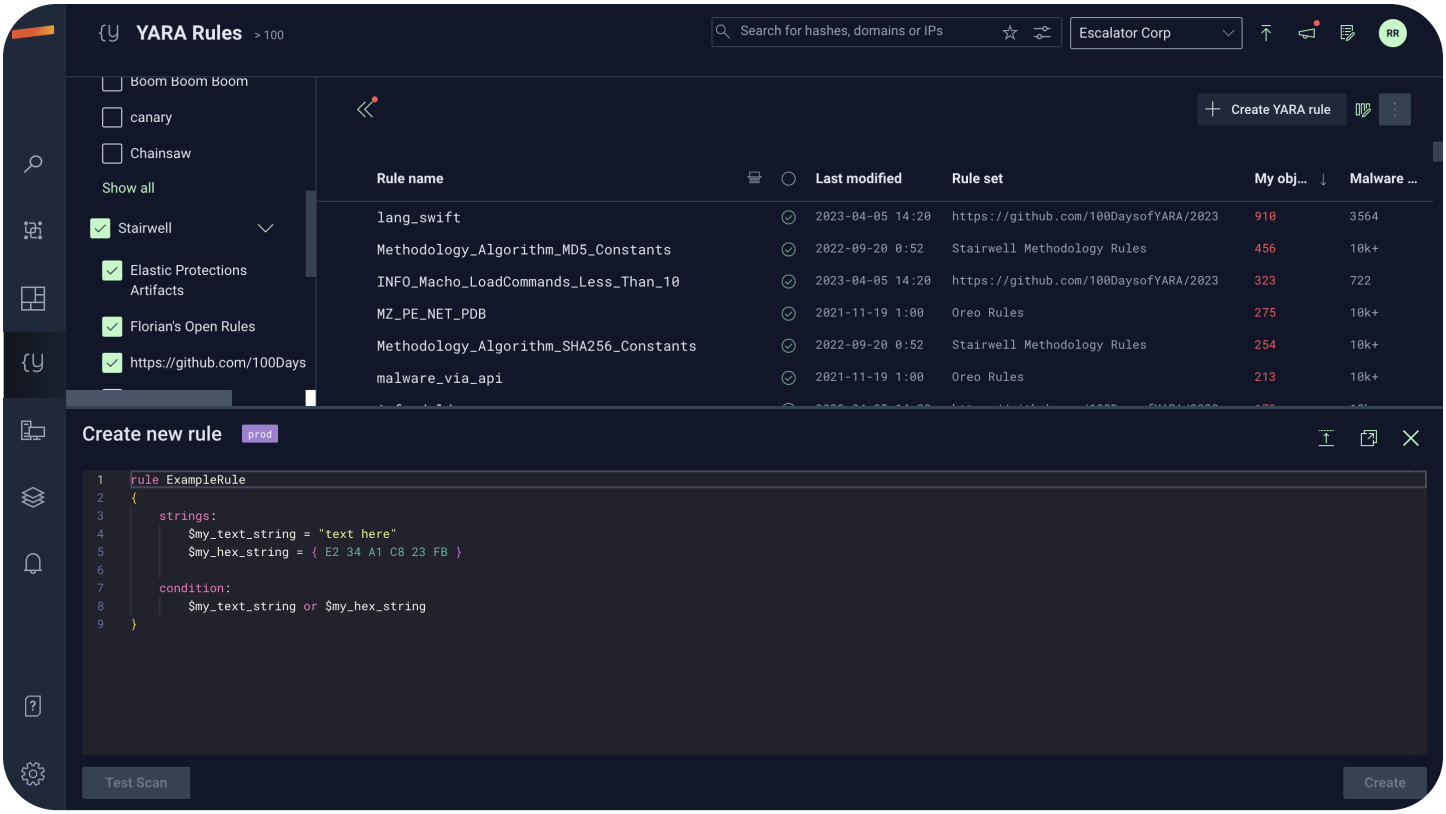
Next level threat hunting

Proactively finding the unknown

As a reminder for those who do not threat hunt day-to-day, at its core, threat hunting is a proactive approach that searches for unknown threats across the different environments within an organization. Think of threat hunting as an insurance policy for your organization. This is because effective threat hunting is able to dramatically improve your chances of spotting and removing undetected threat activity tied to malicious artifacts and behaviors that are not found by existing threat detection solutions.

A whole new approach to threat hunting with Stairwell

Stairwell's unique approach to the problem facing threat hunters is based upon files being the source of truth when it comes to an attack. Stairwell automatically ingests all of your executable-related files and stores them for you forever, resulting in Stairwell helping to take the complexity out of having to find ways to define and apply detailed queries to uncover the unknown. Stairwell analyzes every file at the binary level and automates the hunting process by continuously ingesting all of your threat feeds and extracts all IOCs. In a matter of minutes Stairwell runs a full query across all of your binary files, now or from the past; any matches or discovered variants are presented to the hunt team to investigate and take immediate action.



Next level threat hunting

Your threat hunting team is able to conduct detailed hunts at the code level without worrying about limited resources or retention restrictions. With 4,200+ defined YARA rules and an easy to use query builder, your team is able to both define and test queries that will allow them to continuously hunt to identify patterns across every file within your private cloud instance of Stairwell.

Gone are the restrictions of endpoint performance degradation tied to running queries!

“Structuring” the unstructured to find the unknown
Looking at signals to find the unknown threat or identify something that just seems “off,” requires being able to ask the right questions with the supporting logic and tools to conduct an unstructured hunt. This could be based upon a hunch, analysis of the latest identified threat, or you are simply looking to find something that is not “normal.”

Examples of threat hunting questions and predefined queries within Stairwell include topics such as:

- where files are located or shouldn’t be located
- are there uncommonly deleted executables
- were extensions installed when they shouldn’t have been
- which programs are kicking off at start-up
- which executable files are low in prevalence but are suspicious

Stairwell gives your threat hunters, regardless of level of expertise, a leg up in the never ending game of cat and mouse. Your threat hunting team can quickly identify the unusual or unknown with automated IOC lookups and YARA rules and they can quickly identify suspicious behaviors with the supporting artifacts in order to take action.

To learn how your threat hunting and security teams can stay ahead of even the most advanced threats with the latest technology from Stairwell, please visit www.stairwell.com.