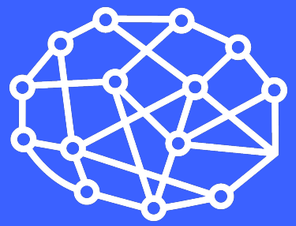
VIRUSTOTAL 2019 ROADMAP

Holistic threat profiling • World class threat hunting • Next generation API and UI

VirusTotal is the **nexus of the security industry.** We **coordinate and empower distributed security teams** to jointly improve security for billions of users.



Holistic threat profiling

World class threat hunting and searching

Next generation API and UI

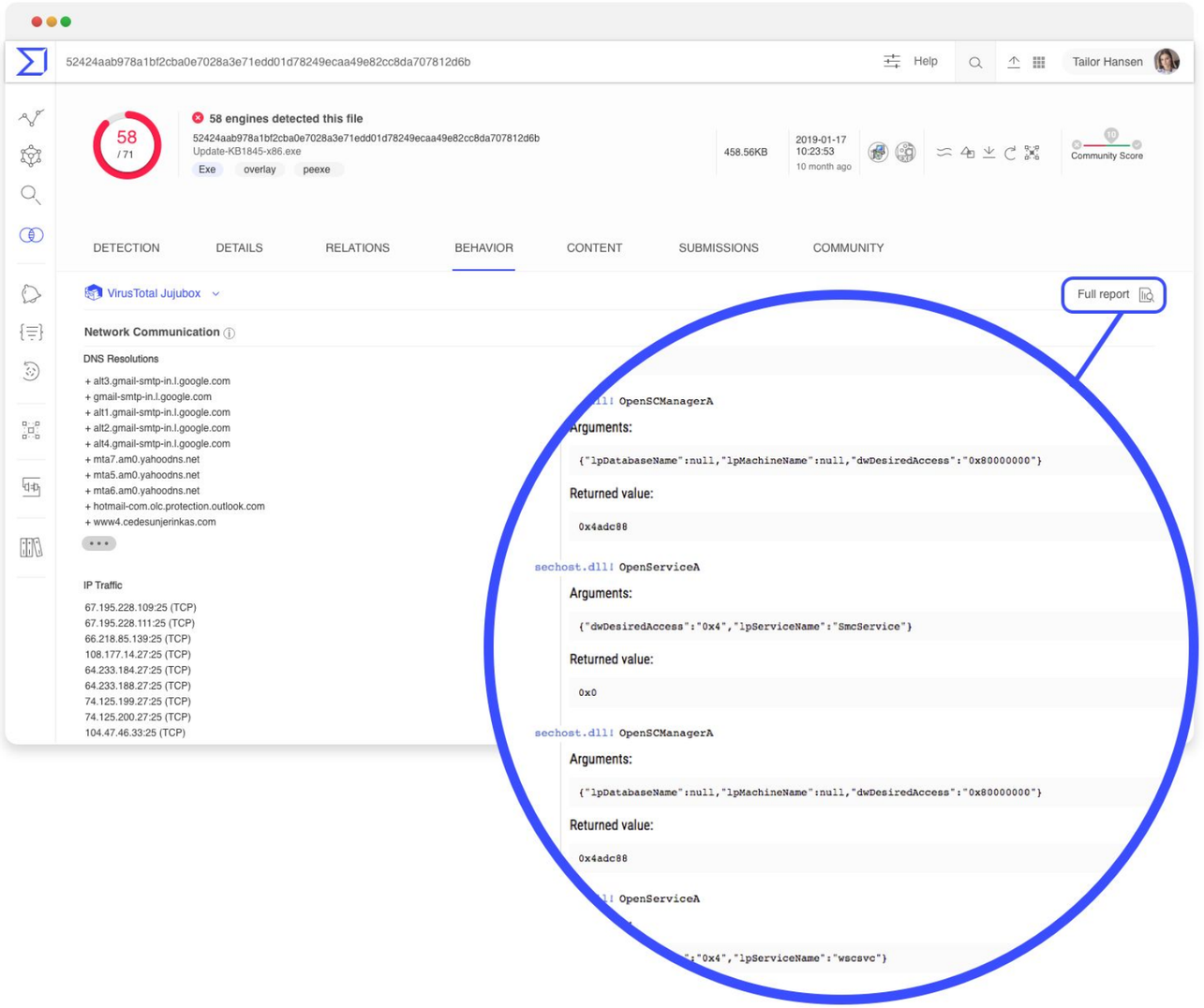
HOLISTIC THREAT PROFILING

Deep characterization of any kind of threat and campaign observable, expand focus beyond files and antivirus verdicts.

World largest dynamic analysis deployment

Nextgen in-house windows sandbox to complement cuckoo fork effort and 5+ new partners contributing to the multisandbox project.

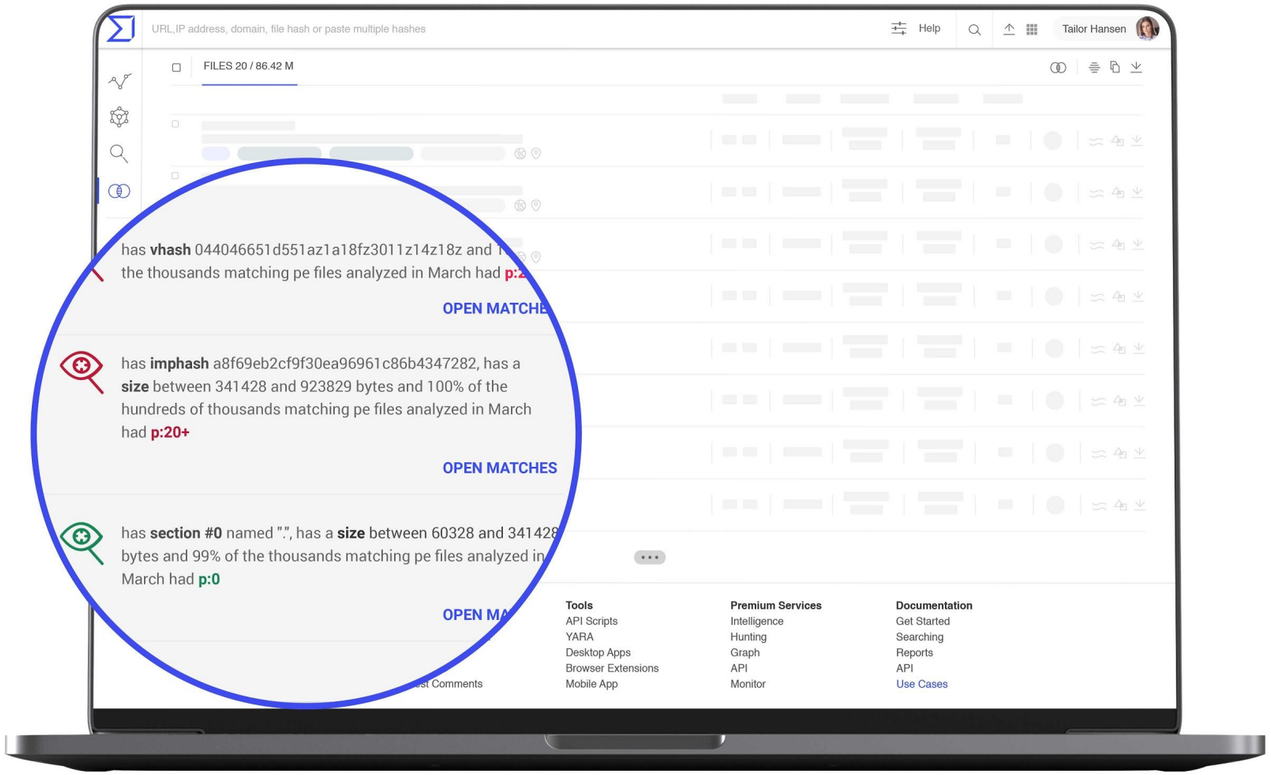
Full revamp of VT's dynamic analysis capabilities, not only focusing on execution traces but also running static+dynamic analysis plugins to decode RAT malware configs and extract network infrastructure that may have not been observed during real time execution.



ML-driven highlighting of suspicious attributes

Enhance heuristics, clustering and pivoting by automatically surfacing properties that are shared by both malicious and harmless files.

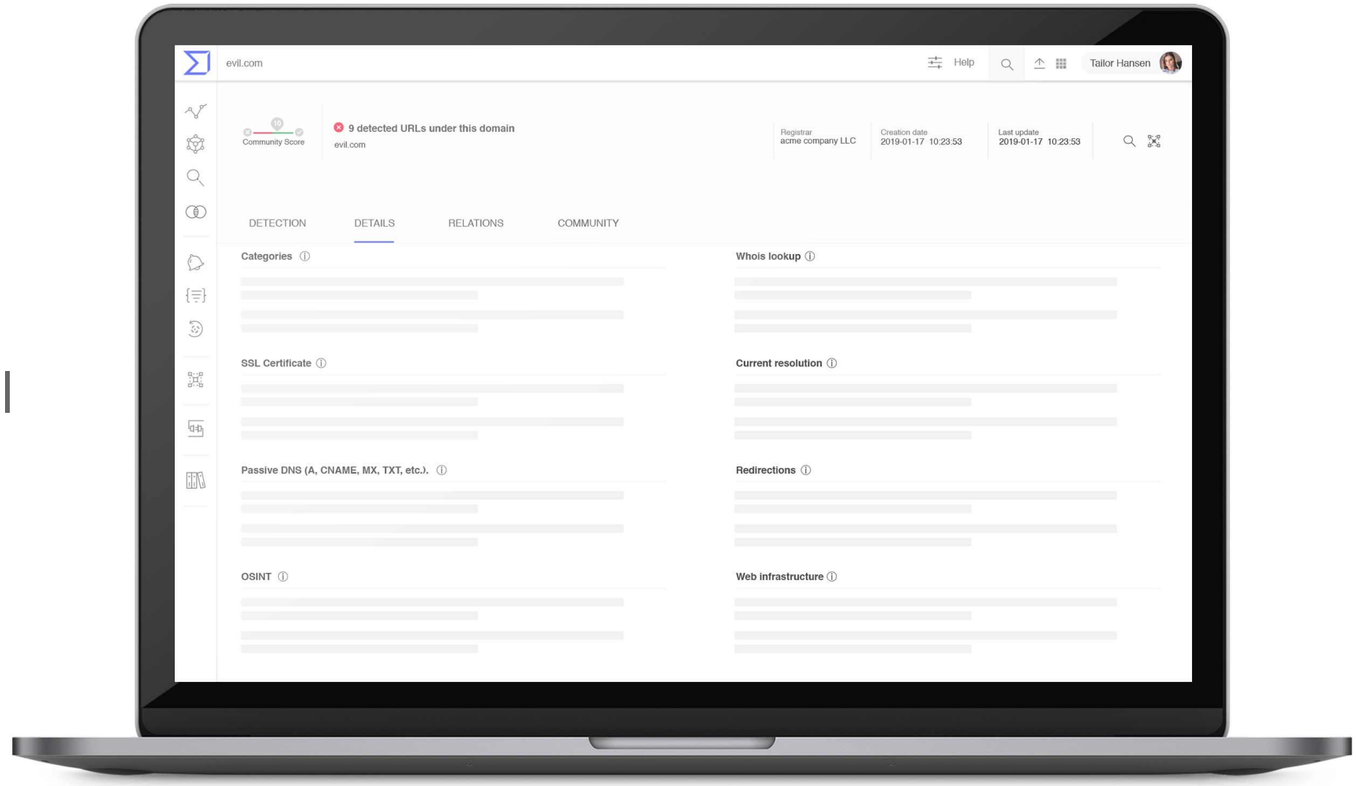
Machines are far better than humans at spotting patterns, patterns that can then be used to find other variants of an attack or to build better defenses against a given threat actor.



Expanded network indicators

Use VT as your single platform to investigate adversaries by aggregating all possible data about domains, IPs and URLs, and of course, files.

Grow beyond passive DNS, historical relationship observations. Inclusion of and pivoting over WHOIS, website content, website trackers, cookies, historical resolutions other than A records, resolution attributes such as TTLs, SSL certificate details, etc.



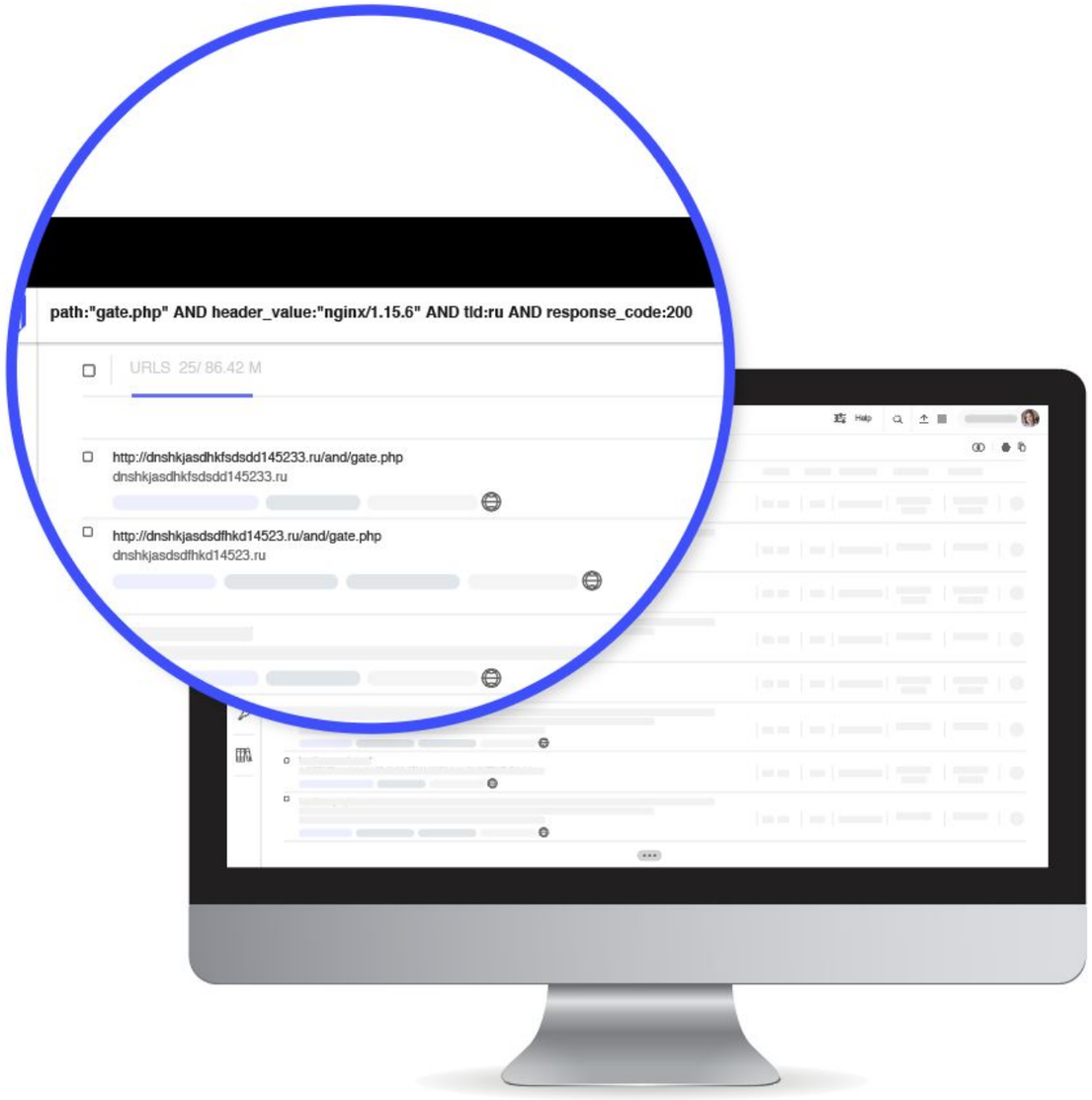
WORLD CLASS THREAT HUNTING AND SEARCHING

Discover attacks and surface adversary infrastructure and artefacts quickly and easily, no matter your field expertise.

Advanced faceted searches over network observables

Discover malicious network infrastructure flying under the radar and pinpoint all the network IoCs (IPs, Domains, URLs) tied to a given attacker or campaign.

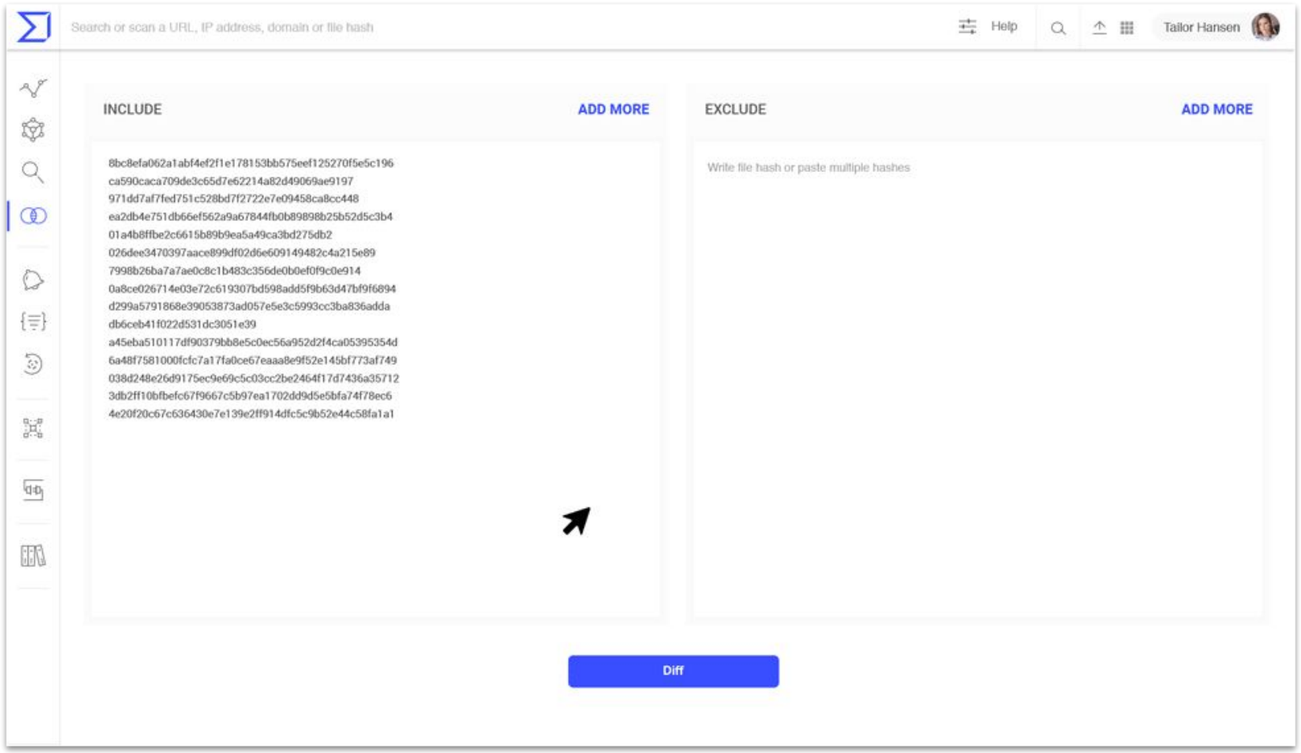
VT Intelligence allows you to perform advanced modifier-based searches over file metadata, content, relationships, behavior, static properties, etc. We are extending this functionality to cover ip addresses, domains and URLs.



Automatic YARA rule generation

Easily and quickly build Yara rules to track a malware family or threat actor, no malware reverse engineering knowledge required.

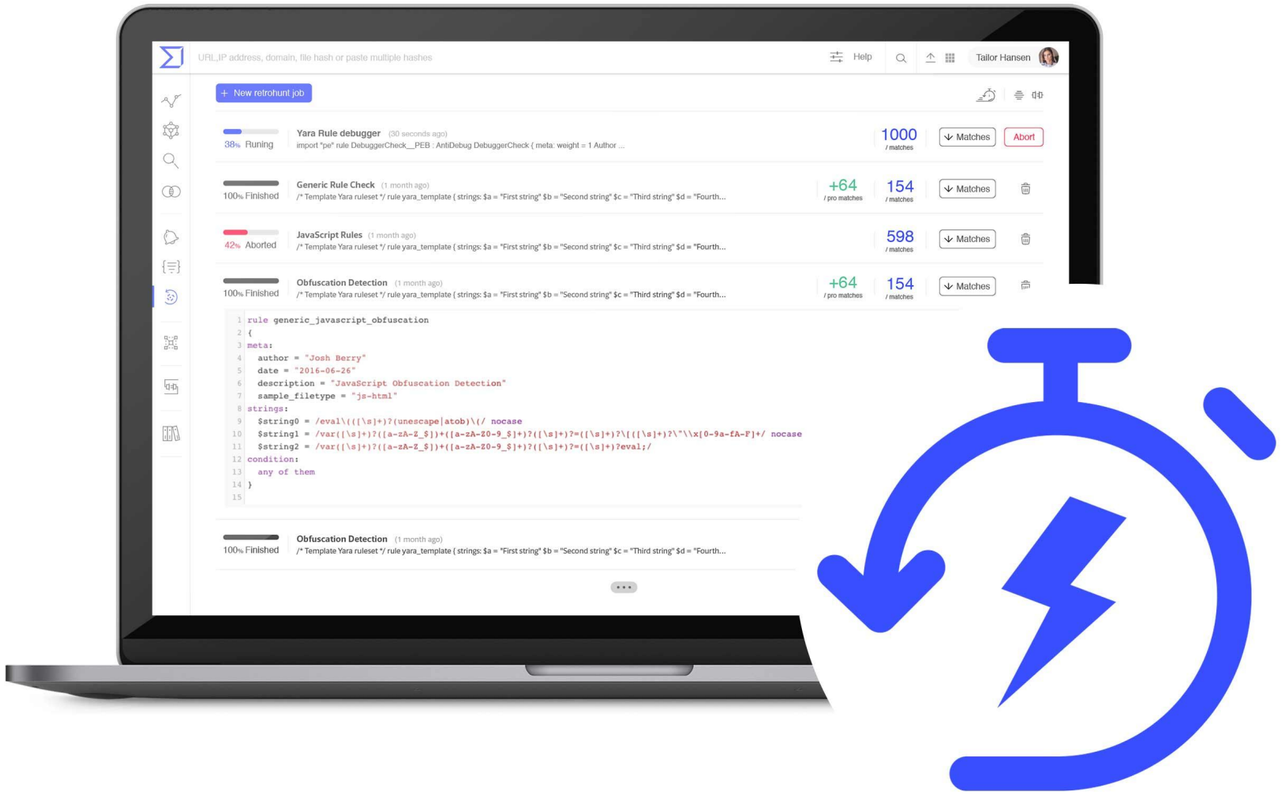
Given a collection of files, automatically generate an optimal rule that will cover your collection and will not produce false positives. Use VT's historical dataset to discard noisy patterns. Leverage this functionality as a first approximation to binary similarity search.



Lightning fast retrohunt

Immediately discover the first variant of an attack or map an entire campaign by matching YARA rules against VT's historical file corpus in under a minute.

Power VTGREP-friendly Retrohunt jobs via VT Intelligence's n-gram content search (VTGREP) to transform a Retrohunt job from being a slow mapreduce task to a fast index lookup. Provided that the YARA rule can be expressed as an n-gram index lookup, execution time goes from hours to under a minute.



NEXT GENERATION API AND UI

Power-up your SOAR flows with advanced threat enrichment beyond AV verdicts and leverage our UIs to automatically assist and guide your investigations.

VT GRAPH expansion playbooks

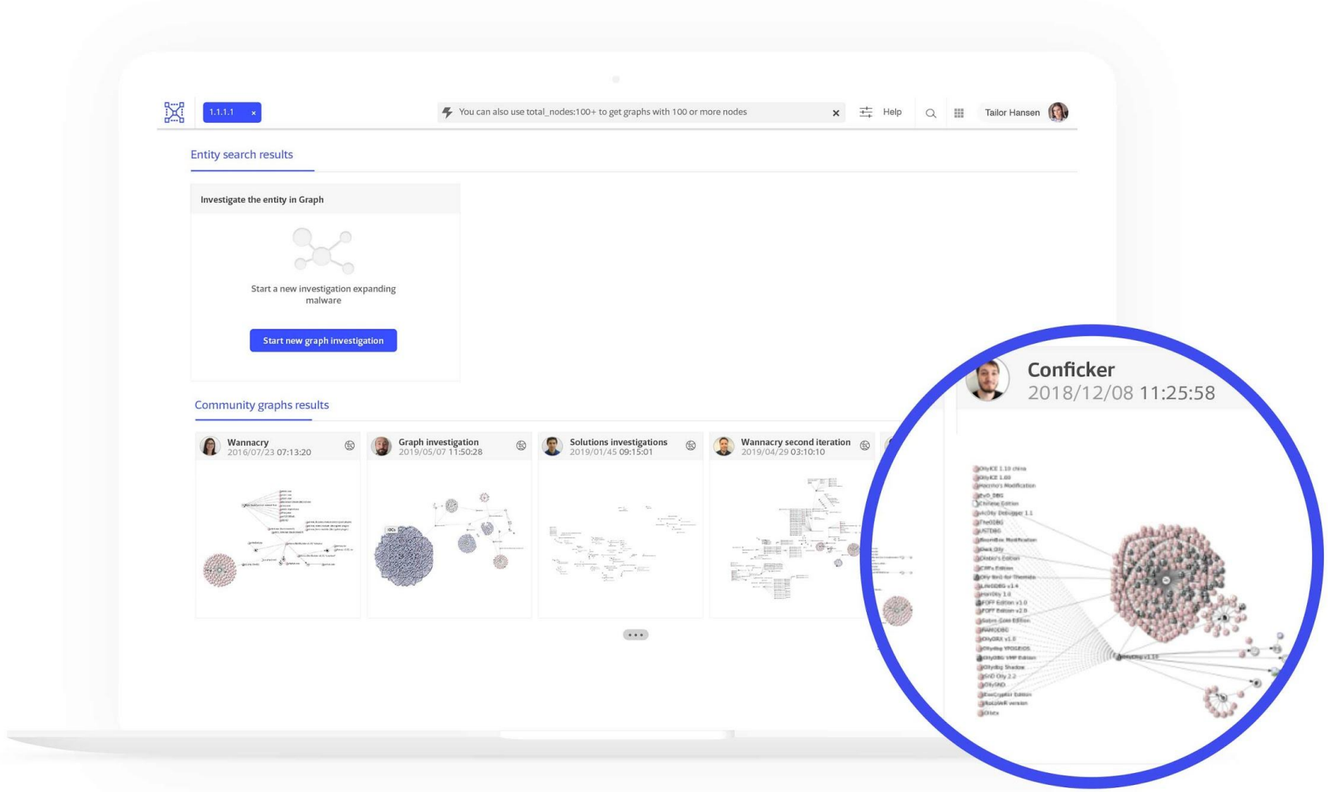
Discover all the infrastructure and artifacts used in a campaign or operated by a threat actor by automating relationship exploration and pivoting in VT Graph.

Store and run playbooks specifying depth and relationship type expansions to automatically generate a threat graph given an initial set of observables, uncover badness quickly and easily.

Advanced faceted searches over stored VT GRAPHs

Enrich your knowledge about adversaries by easily filtering historical internal and community investigations that exhibit ties to a given observation.

VT Intelligence-like searches over stored graphs, both private and public. For instance, search for all those graphs that display communication with domain *evil.com* and contain an email file type node.



Unprecedented threat context and discovery via API v3

Programmatically power-up your investigations by leveraging 15+ years of historical threat observations via APIv3.

Comprehensive threat data beyond AV verdicts. Relationships oriented, programmatically map artefacts related to an observable. Nextgen sandbox file detonation reports. Programmatic VTHUNTING workloads. Extended restrospection windows via Threat Hunter PRO.