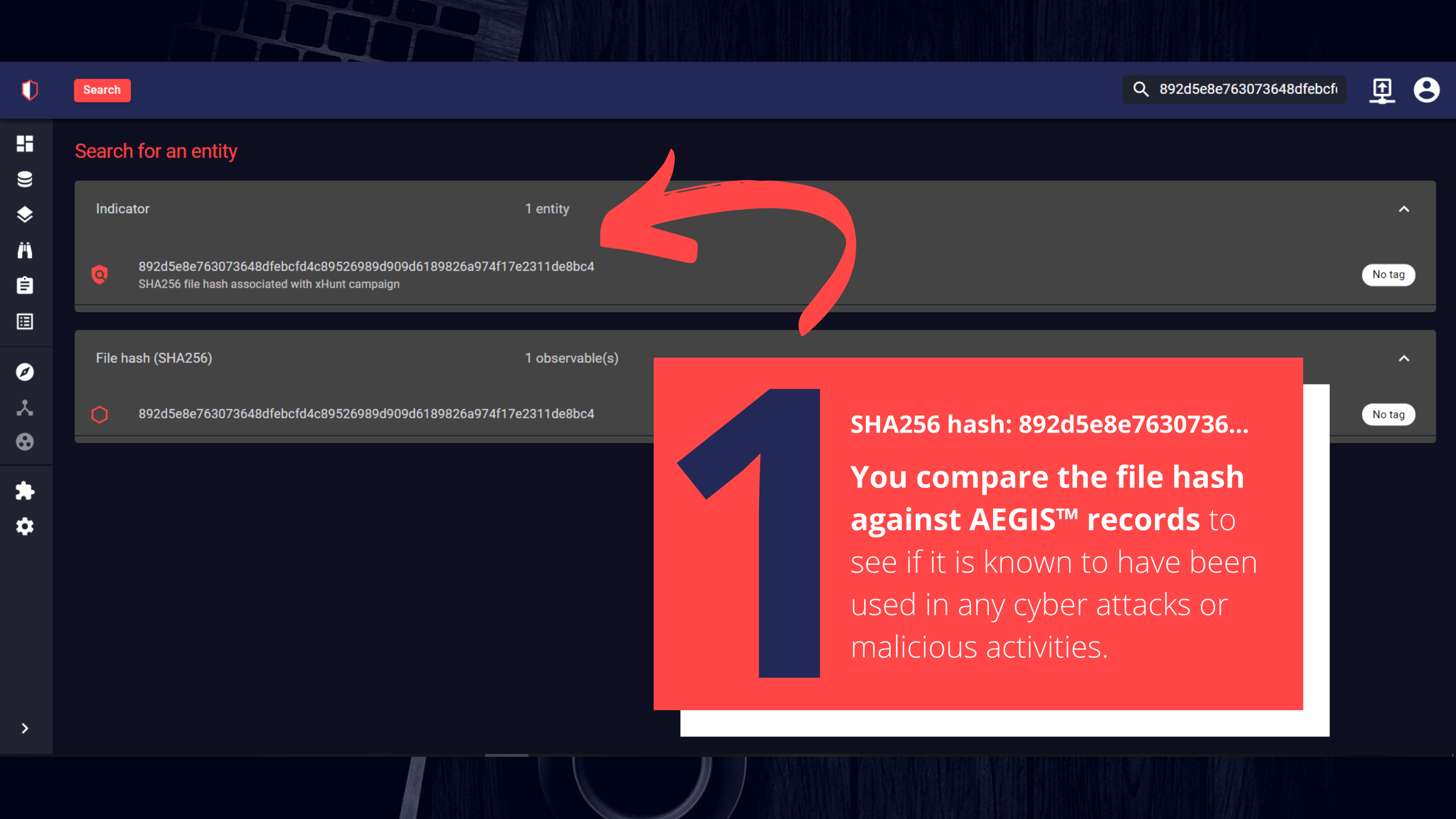
2020 EDITION

AEGIS™

SECURITY ANALYST: AN ADVANCED PERSISTENT THREAT USE CASE

YOU ARE

A Security Analyst at a large organization operating in the logistics sector. The IDS system identified malicious activity on one of the servers caused by an executable ran today. You produce a hash of the file in question and turn to AEGIS™ to analyze the file's origins.


Search
892d5e8e763073648dfebcf
Search for an entity
Indicator
1 entity
892d5e8e763073648dfebcfd4c89526989d909d6189826a974f17e2311de8bc4
SHA256 file hash associated with xHunt campaign
No tag
File hash (SHA256)
1 observable(s)
892d5e8e763073648dfebcfd4c89526989d909d6189826a974f17e2311de8bc4
No tag
1
SHA256 hash: 892d5e8e7630736...
You compare the file hash against AEGIS™ records to see if it is known to have been used in any cyber attacks or malicious activities.

Indicators > Overview Observables

Search...

892D5E8E763073648DFEBCFD4C89526989D909D6189826A974...

TLP:WHITE

Information

Pattern type
stix

Creation date
February 20, 2020

Modification date
February 20, 2020

Creator
ALIENVAULT

Description
SHA256 file hash associated with xHunt campaign

Details

Indicator pattern

```
[file:hashes.SHA256 =
'892d5e8e763073648dfebcfd4c89526989d909d6189826a974f17e2311de8bc4']
```

Valid from
February 20, 2020

Valid until
February 19, 2021

Score
50/100

Tags +

Last reports about the entity

2

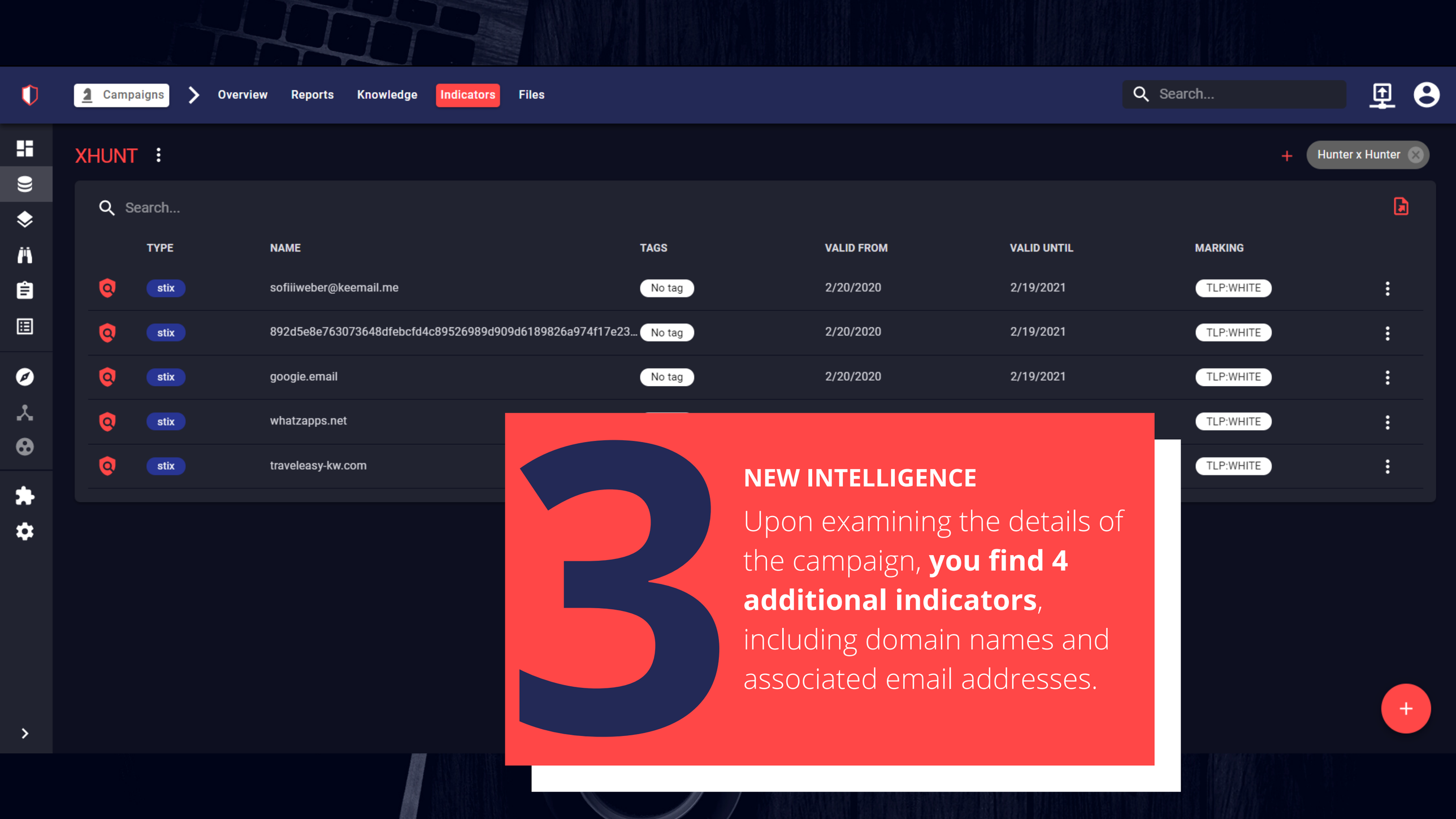
ON THE HUNT

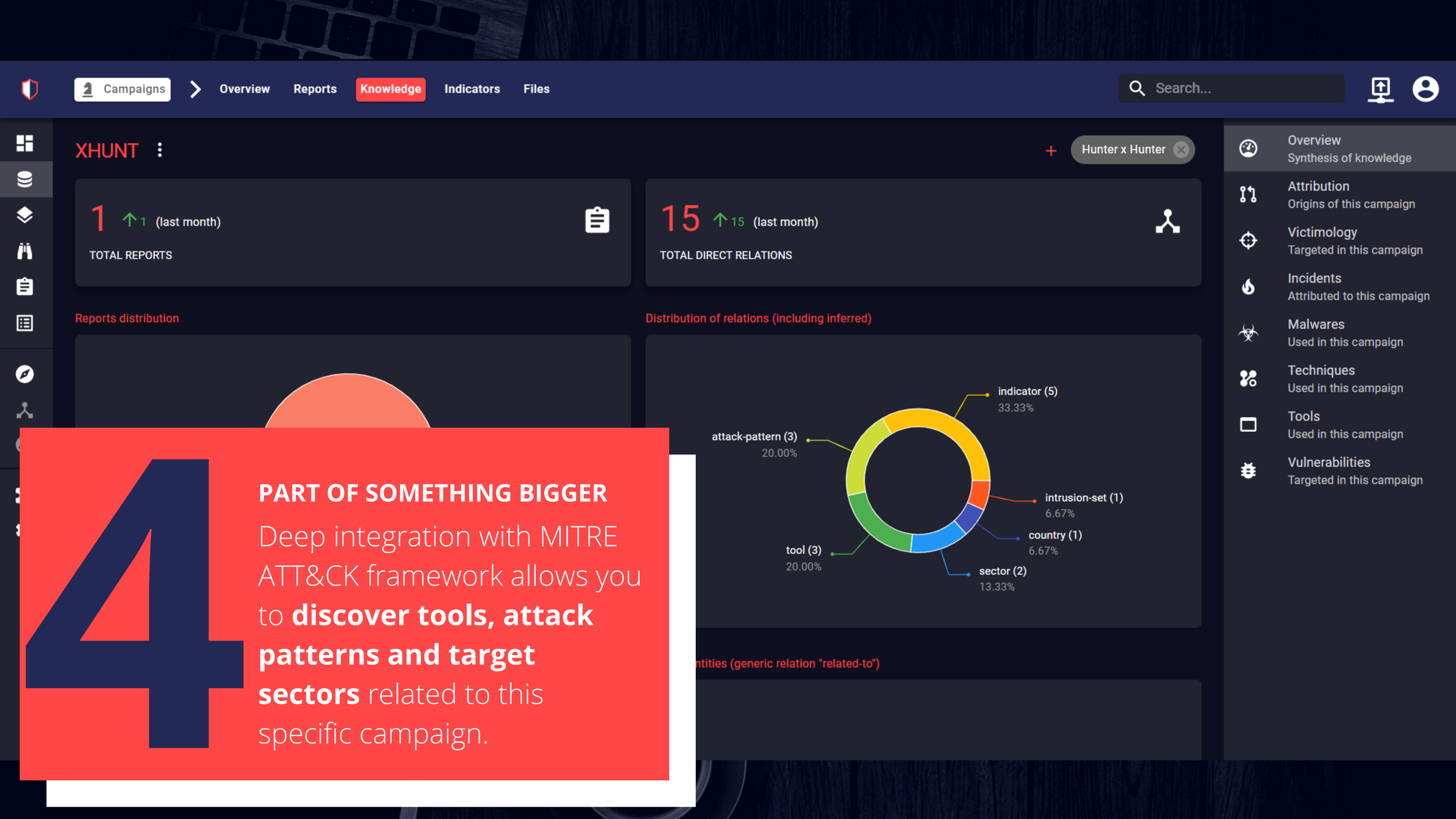
After expanding the details about the indicator, you discover a strong connection with **an existing malware campaign**.

Relations to threats +

Search...

ENTITY TYPE	NAME	LAYED ROLE	FIRST OBS.	LAST OBS.	CONFIDENCE
Campaign	xHunt	Unknown	5/1/2019	2/20/2020	Strong

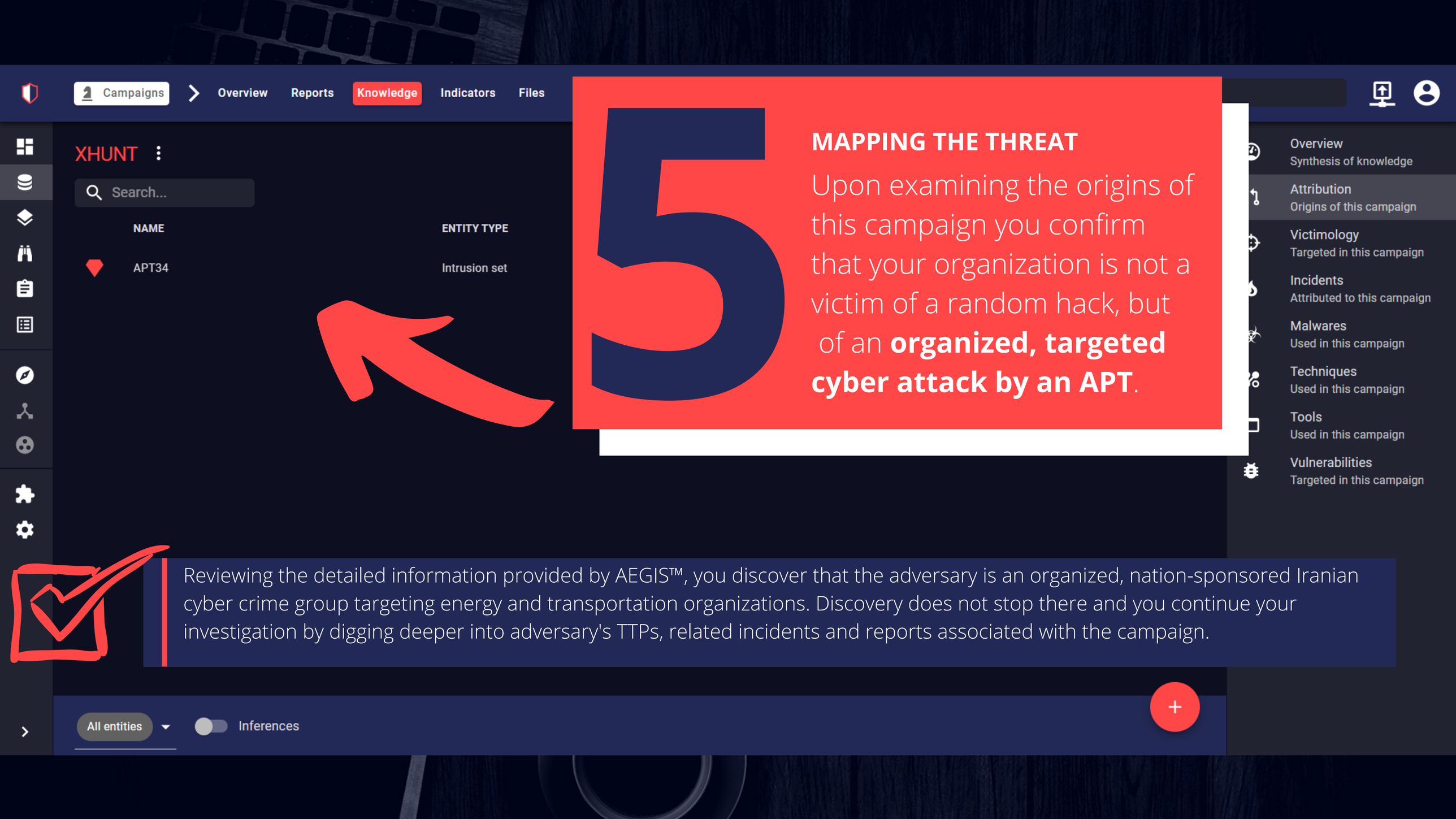

Campaigns
Overview
Reports
Knowledge
Indicators
Files
Search...
XHUNT
Hunter x Hunter
Search...
TYPE
NAME
TAGS
VALID FROM
VALID UNTIL
MARKING
stix
sofiiiweber@keemail.me
No tag
2/20/2020
2/19/2021
TLP:WHITE
stix
892d5e8e763073648dfebcfd4c89526989d909d6189826a974f17e23...
No tag
2/20/2020
2/19/2021
TLP:WHITE
stix
googie.email
No tag
2/20/2020
2/19/2021
TLP:WHITE
stix
whatzapps.net
TLP:WHITE
stix
traveleasy-kw.com
TLP:WHITE
3
NEW INTELLIGENCE
Upon examining the details of the campaign, you find 4 additional indicators, including domain names and associated email addresses.

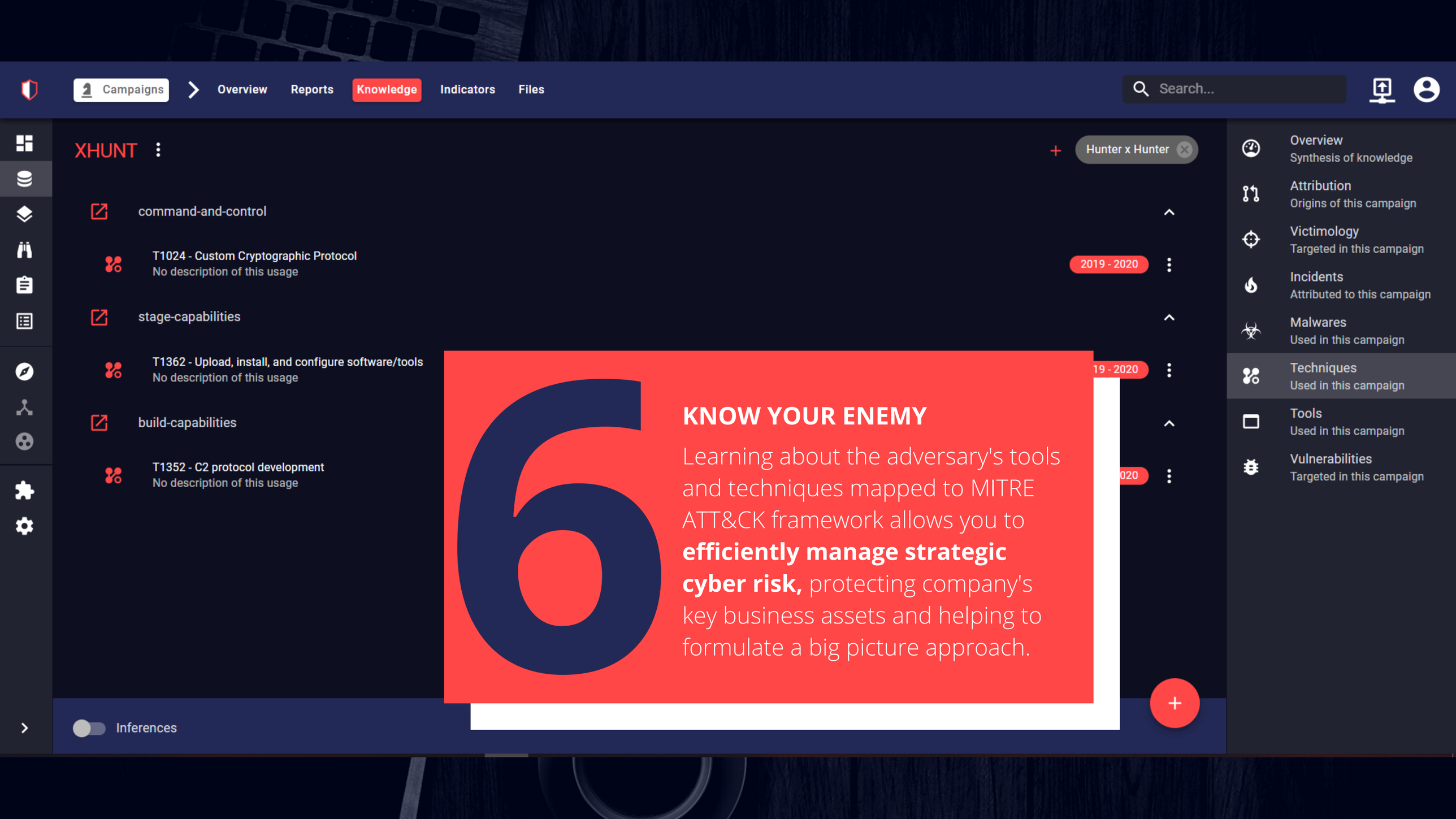


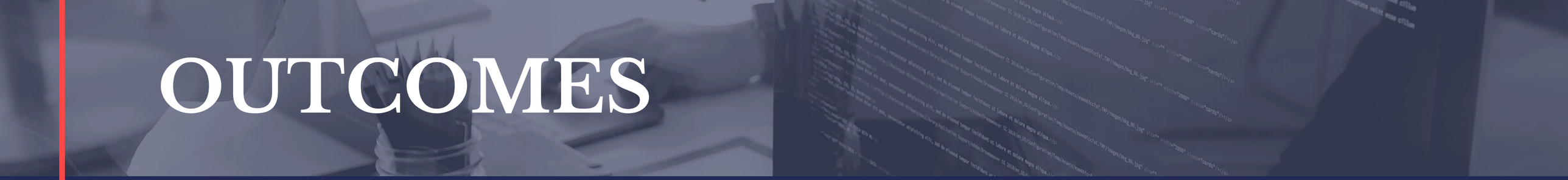
4

PART OF SOMETHING BIGGER

Deep integration with MITRE ATT&CK framework allows you to **discover tools, attack patterns and target sectors** related to this specific campaign.


Campaigns
Overview
Reports
Knowledge
Indicators
Files
XHUNT
Search...
NAME
ENTITY TYPE
APT34
Intrusion set
5
MAPPING THE THREAT
Upon examining the origins of this campaign you confirm that your organization is not a victim of a random hack, but of an organized, targeted cyber attack by an APT.
Overview
Synthesis of knowledge
Attribution
Origins of this campaign
Victimology
Targeted in this campaign
Incidents
Attributed to this campaign
Malwares
Used in this campaign
Techniques
Used in this campaign
Tools
Used in this campaign
Vulnerabilities
Targeted in this campaign
Reviewing the detailed information provided by AEGIS™, you discover that the adversary is an organized, nation-sponsored Iranian cyber crime group targeting energy and transportation organizations. Discovery does not stop there and you continue your investigation by digging deeper into adversary's TTPs, related incidents and reports associated with the campaign.
All entities
Inferences


Campaigns
Overview
Reports
Knowledge
Indicators
Files
Search...
XHUNT
Hunter x Hunter
command-and-control
T1024 - Custom Cryptographic Protocol
No description of this usage
2019 - 2020
stage-capabilities
T1362 - Upload, install, and configure software/tools
No description of this usage
19 - 2020
build-capabilities
T1352 - C2 protocol development
No description of this usage
020
Inferences
Overview
Synthesis of knowledge
Attribution
Origins of this campaign
Victimology
Targeted in this campaign
Incidents
Attributed to this campaign
Malwares
Used in this campaign
Techniques
Used in this campaign
Tools
Used in this campaign
Vulnerabilities
Targeted in this campaign
6
KNOW YOUR ENEMY
Learning about the adversary's tools and techniques mapped to MITRE ATT&CK framework allows you to **efficiently manage strategic cyber risk,** protecting company's key business assets and helping to formulate a big picture approach.



OUTCOMES

- Early incident containment and eradication due to centralized IoCs and campaign info.
- Adversary and their TTPs identified and mapped to MITRE ATT&CK, enabling threat modelling and reducing strategic risk.
- Straightforward reporting due to export features and associated external reports.

ENABLING SECURITY OPS

Whether your organization has a Security Operations Centre setup already, or is starting a cyber threat management component from scratch, AEGIS™ provides a cost-effective centralized threat intelligence management solution, **multiplying the efficiency of your security team** with great ROI.

HOLISTIC THREAT IDENTIFICATION

Everything in AEGIS™ is connected through dynamic relationships, allowing you to grasp the full picture immediately and respond to an incident in a timely manner.

EFFICIENT INCIDENT TRIAGE

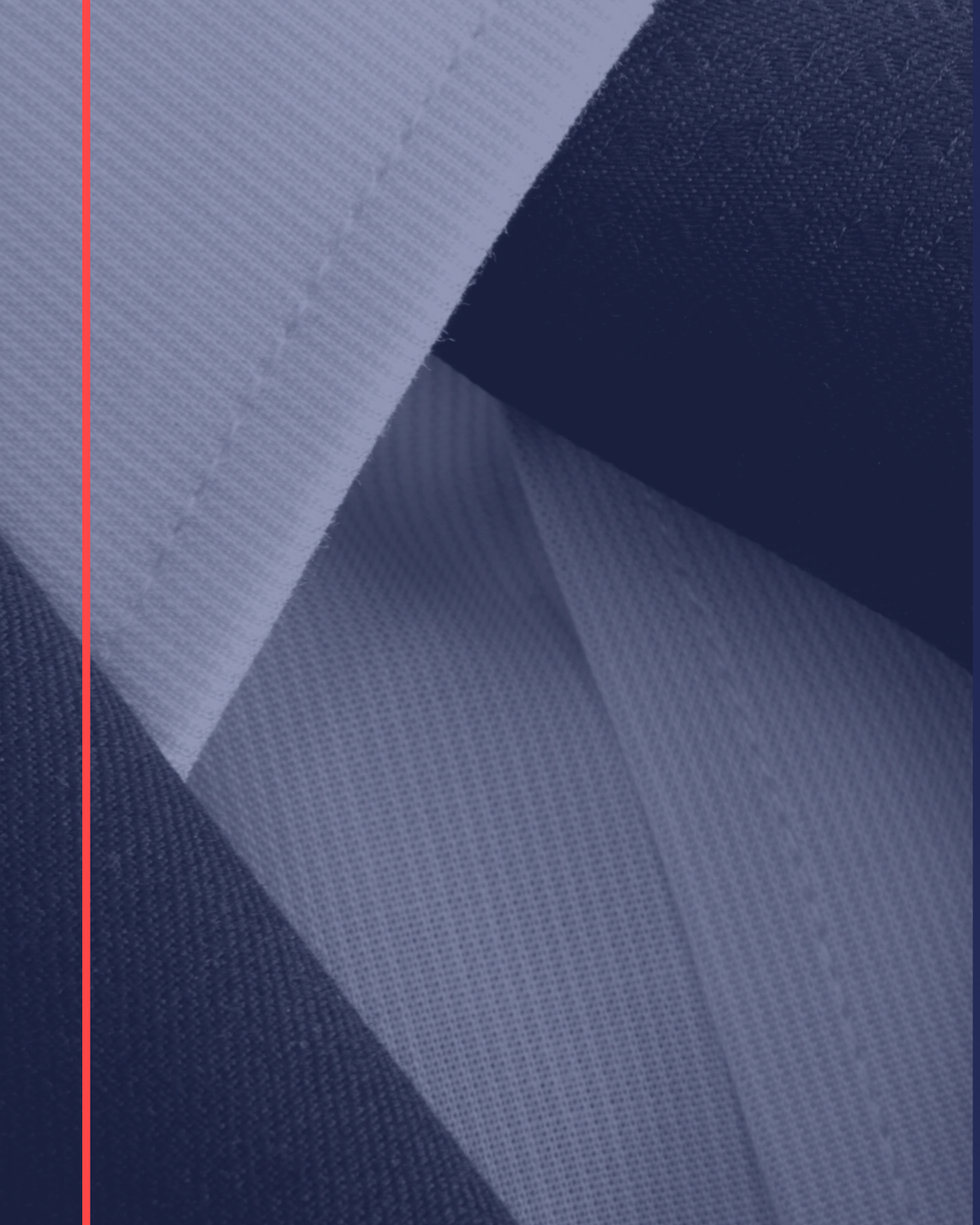
Our analysts are happy to work with you 24/7 and will help you get the maximum benefit out of the platform through training, support, crisis simulation and incident response assistance.

ONE STOP SHOP FOR YOUR CTI NEEDS

Indicators, reports, campaigns, threat actors, forensic graph analytics and scenario analysis - all of this and more in one place, allowing you to make AEGIS™ your top threat management platform.

NEAR REAL TIME UPDATES

AEGIS™ receives a constant feed of open and closed collection sources, processing over 1000 data points per second. With an evolving landscape, AEGIS™ is built to evolve with the threats we face.



ASK FOR MORE

ADDRESS

340 King Street East, 4th Floor, Toronto, Ontario

PHONE

647-952-0920

EMAIL

info@wembleypartners.com