VEDERE LABS

Threat Feeds & Lookup Service

Continuous, real-time determination of malicious activity

Vedere Labs is providing a **service** to share threat intel with third parties in machine readable format.

We can share:
- **Indicators of compromise (IoCs)** that include malicious **URLs**, malware **hashes** and **malicious email and IP addresses** related to attacks
- **Context-enriched threat information** (e.g., which verticals are impacted by a given vulnerability or what threat actor is associated to a given bad IP)

How we are different

- Focus on **OT/IoT/IoMT**
- Focus on the **network** + the **device** (and not only endpoints)

THREAT FEEDS

Our cybersecurity researchers **constantly monitor** the threat landscape to generate timely and valuable threat feeds via:

- Original **vulnerability research** activities

- Manual and automatic analysis of **malware samples collected on the ground**

- Manual and automatic analysis of **malicious behavior** observed

- Malicious activities observed over the networks of anonymized **Forescout customers**

- **Partnerships** with the community and universities

USE CASES

Original Threat Intelligence in Our Products

Forescout Continuum can consume original, home-grown threat intel

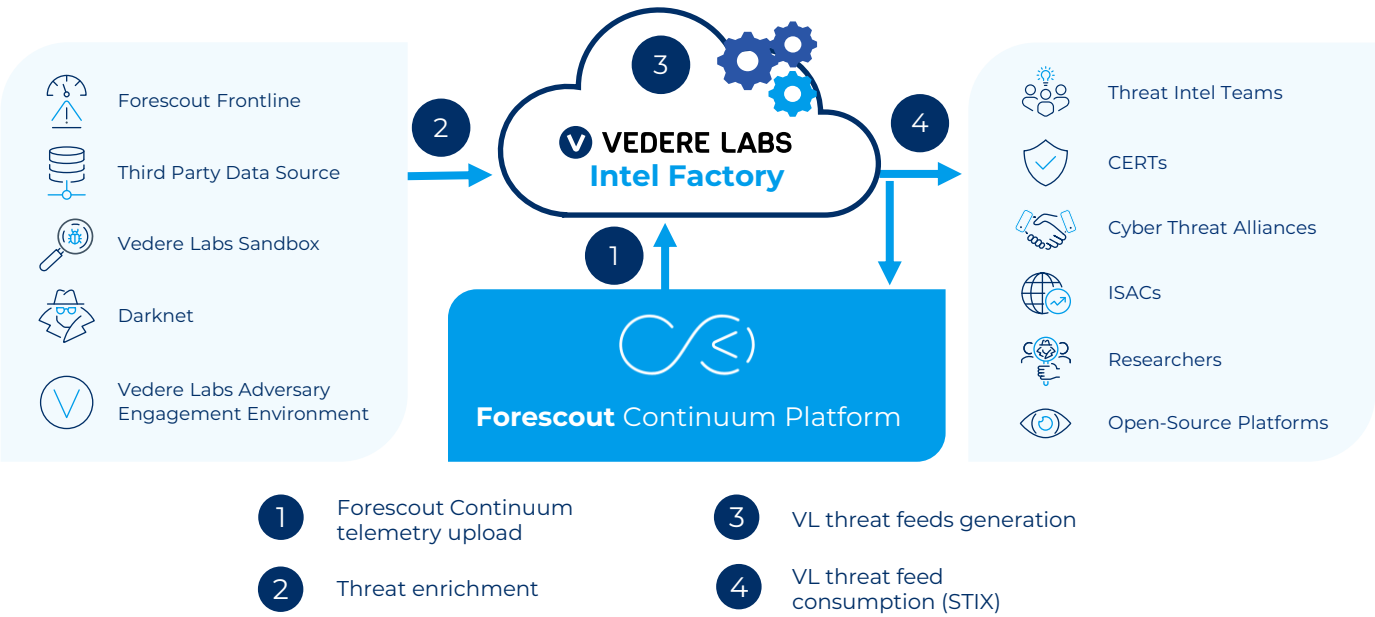### Collaborative Threat Intelligence

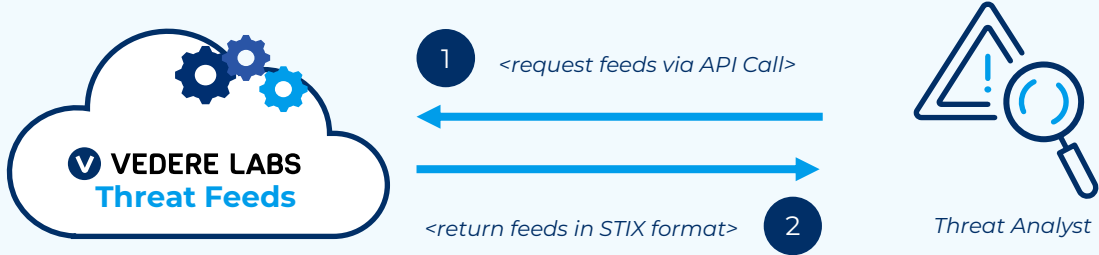Share intelligence with governments, ISACs and threat alliances

Lookup & Enrichment Service

Query our unique threat knowledge base to validate hypotheses and gain insights
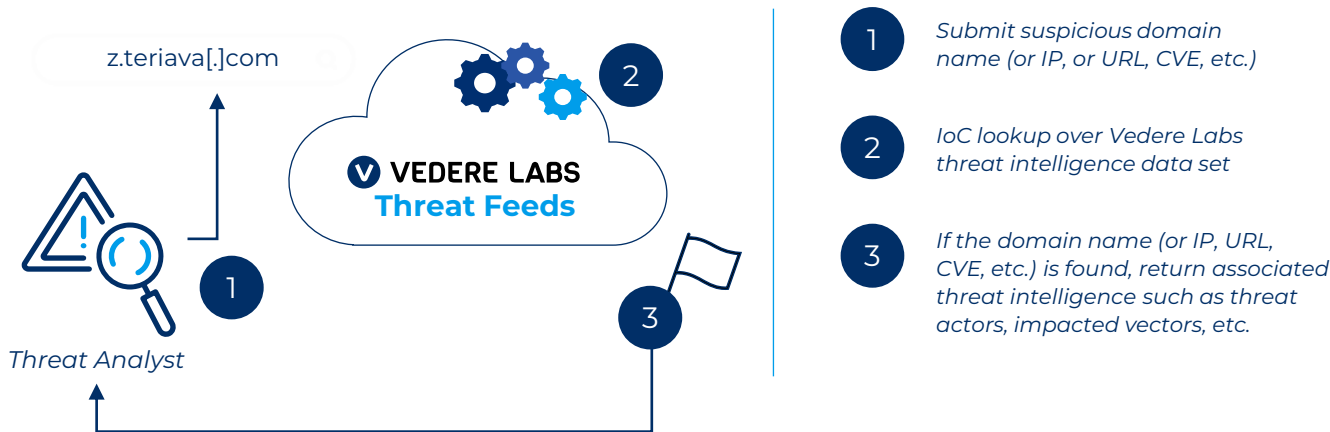
HOW VEDERE LABS GENERATES ORIGINAL THREAT FEEDS

Forescout Frontline

Third Party Data Source

Vedere Labs Sandbox

Darknet

Vedere Labs Adversary
Engagement Environment

V VEDERE LABS
Intel Factory

Forescout Continuum Platform

Threat Intel Teams

CERTs

Cyber Threat Alliances

ISACs

Researchers

Open-Source Platforms

1 Forescout Continuum
telemetry upload

2 Threat enrichment

3 VL threat feeds generation

4 VL threat feed
consumption (STIX)

THREAT FEED SERVICE

V VEDERE LABS
Threat Feeds

1 *<request feeds via API Call>*

<return feeds in STIX format> 2

Threat Analyst

THREAT LOOKUP SERVICE

The **Vedere Labs Threat Lookup Service** allows real-time determination of malicious domain names by using an *algorithm that can predict if a domain name is malicious, even if it has never been seen before*. The resulting disposition is returned to the request along with specific threat actors, malware or active campaigns associated with it.

z.teriava[.]com

V VEDERE LABS
Threat Feeds

Threat Analyst

1 *Submit suspicious domain name (or IP, or URL, CVE, etc.)*

2 *IoC lookup over Vedere Labs threat intelligence data set*

3 *If the domain name (or IP, URL, CVE, etc.) is found, return associated threat intelligence such as threat actors, impacted vectors, etc.*

1. Go to feeds.vederelabs.com

2. Register

3. Wait for approval and token release

4. Login

6. Ready to go!

5. Read the documentation to start using the service

<) FORESCOUT®

V VEDERE LABS